المسؤولية المدنية الناشئة عن معالجة البيانات الشخصية الرقمية

م.د. كوثر فاضل جاسم
وزارة التعليم العالي والبحث العلمي/ دائرة الدراسات والتخطيط والمتابعة
kawtherfadhil83@gmail.com

Civil liability arising from the processing of digital personal data

Kawthar Fadal jasem Al Sudani
Workplace - Ministry of Higher Education and Scientific Research/Department of Studies and Planning

المقدمة

في ضوء التوسع الهائل في استخدام الوسائط الرقمية، وما يرتبط بها من تزايد مضطرد في المعالجات الإلكترونية للبيانات الشخصية، يواجه النظام القانوني الحديث تحديات غير مسبوقة تمس جوهر العلاقة بين الفرد والسلطة، بين الخصوصية والتقنية، وبين الحقوق التقليدية والأدوات الحديثة لانتهاكها. فالمجتمع الرقمي لم يخلق فقط فضاءً افتراضيًا جديدًا، بل أعاد تشكيل حدود الذات القانونية، إذ بات من الممكن رصد، تحليل، واستغلال كل أثر رقمي يتركه الإنسان أثناء تفاعله مع محيطه التكنولوجي، مما يجعل البيانات الشخصية ـــ الرقمية منها على وجه الخصوص . **واحدة من أبرز معالم السيادة الفردية في العصر الحديث**(العيش، 2023، ص. 289).

ويزداد تعقيد الإشكال القانوني عندما تتعرض هذه البيانات، التي تُعد تعبيرًا دقيقًا عن الهوية الإنسانية، لمعالجات غير مشروعة، دون أن يكون لدى الضحية سلاح قانوني ناجز يمكن من خلاله استرداد اعتباره أو التعويض عن الضرر الحاصل.

إذ أن النظم القانونية، لا سيما ذات الطبيعة المدنية، لا تزال . في كثير من بيئاتها . أسيرة نصوص تقليدية صيغت لوقائع مادية محسوسة، كأضرار السيارة أو البناء أو العقود، ولم تتهيأ بعد لمعالجة ظواهر معقدة وغير مرئية، كاختراقات الخصوصية أو تسريب المعطيات أو التتبع الرقمي دون إذن. وهكذا، تظهر **فجوة تشريعية صارخة بين آليات المساءلة التقليدية ومظاهر الضرر الحديث**، في ظل غياب إطار واضح لـــ"المسؤولية المدنية الرقمية" بوصفها فرعًا ناشئًا ومتطلبًا ملحًا (علي، 2023، ص. 229).

وتبدو هذه الفجوة أوضح ما تكون في النظام المدني العراقي، الذي لم يشهد ـــ حتى وقت قريب . تطورًا تشريعيًا يُمكّنه من التعامل مع المعالجة الرقمية للبيانات بوصفها نشاطًا قد يرتب التزامًا بالتعويض، سواء قام به فرد أم جهة عامة أو خاصة. فبينما تنبّهت بعض الدول، كالولايات المتحدة ودول الاتحاد الأوروبي، إلى خطورة انفلات المعالجة من قيد القانون، وأقرت قواعد نوعية تضبط العلاقة بين المعالِج والبيانات، وتمنح صاحب الحق أدوات قانونية فاعلة للمطالبة بجبر الضرر، لا يزال

الخطاب القانوني العربي عمومًا، والعراقي تحديدًا، يعتمد أدوات تكييفية محدودة في توصيف هذا النوع من الانتهاك (براك، 2024، ص. 342).

وفي هذا السياق، تُعد واقعة شركة **Cambridge Analytica** نقطة تحول دولية لافتة. ففي عام 2018، تم الكشف عن استخدام بيانات شخصية لأكثر من **87مليون مستخدم لفيسبوك** دون موافقتهم، في أغراض سياسية وتجارية، مما أدى إلى **تسوية قضائية تاريخية بقيمة 725 مليون دولار أمريكي** ضد شركة (Facebook "Meta"سابقًا) في عام 2022 .(Reuters, 2022)هذه الواقعة لم تكن مجرد انتهاك تقني، بل برهنت على أن **البيانات الشخصية قد تتحوّل إلى أدوات تأثير سياسي، ومصدر ربح غير مشروع، وأساس لانتهاك الخصوصية الجمعية** في غياب حماية قانونية مدنية فعالة.

وتُبرز الإحصائيات الحديثة بدورها حجم الخطر، إذ أفاد تقرير لشركة Varonis (2024) أن **متوسط تكلفة خرق البيانات في الشرق الأوسط بلغ 8.75 مليون دولار**، لتصبح المنطقة ثاني أعلى منطقة عالميًا بعد الولايات المتحدة في هذا المجال. هذه الأرقام تشير إلى هشاشة البنية القانونية في دول الإقليم، وتكشف ضعف التشريعات المدنية في احتواء النتائج الاقتصادية والاجتماعية لمثل هذه المعالجات الرقمية غير القانونية.

وعليه، يُشكّل موضوع "المسؤولية المدنية عن معالجة البيانات الشخصية الرقمية" أحد أبرز الإشكاليات القانونية التي تتطلب دراسة تحليلية متعمقة، تتجاوز السياق الفقهي التقليدي، وتسعى إلى **تفريد نمط جديد من المسؤولية القانونية، يُؤسس على خطأ من طبيعة تقنية، ويقر ضررًا أدبيًا يترتب على اختراق غير محسوس، ويفترض علاقة سببية تتسم بالخفاء والتداخل** .وهذا ما تسعى إليه هذه الدراسة، عبر تحليل مقارن بين القوانين العراقية، المصرية، واللائحة العامة لحماية البيانات الأوروبية(GDPR) ، في محاولة لاستجلاء مدى كفاية الأطر القانونية المدنية في حماية هذا الحق الرقمي الناشئ.

إشكالية البحث : هل تفي قواعد المسؤولية المدنية التقليدية، في قوانين كالقانون المدني العراقي والمصري، بمتطلبات حماية البيانات الشخصية الرقمية من المعالجة غير المشروعة؟ وهل يمكن تطوير تصور قانوني متكامل لمسؤولية مدنية رقمية تستوعب عناصر الخطأ، الضرر، والعلاقة السببية، في السياق الإلكتروني؟

أهمية البحث

1. يعالج **فراغًا تشريعيًا حرجًا في القانون المدني العراقي،** في ظل انفجار التطبيقات الرقمية وتأثيرها العميق على الخصوصية الفردية.
2. يقدم **تفكيكًا منهجيًا لأركان المسؤولية المدنية الرقمية،** في ضوء الاجتهاد المقارن والواقع القضائي الأوروبي والمصري.
3. يُقدّم **أرضية اقتراحية لتطوير القانون المدني العراقي،** بما يسمح له بمسايرة البيئة الرقمية وتوفير حماية حقيقية غير شكلية للبيانات الشخصية.

أهداف البحث

- رسم الإطار القانوني الدقيق لمفهوم **البيانات الشخصية الرقمية** وضوابط معالجتها.
- تحديد مدى توافر أركان المسؤولية المدنية في سياق المعالجة الرقمية للبيانات.
- تحليل الموقفين المصري والأوروبي، واستنباط قواعد يمكن تبنيها لصياغة مسؤولية مدنية رقمية عراقية.

منهجية البحث **يعتمد البحث على:**

1. **المنهج التحليلي** :لاستقراء النصوص القانونية وتفسير الفقه المتعلق بالمسؤولية المدنية.
2. **المنهج المقارن** :عبر دراسة موقف القانونين العراقي والمصري، مقابل اللائحة الأوروبية العامة لحماية البيانات.
3. **المنهج التطبيقي** :من خلال دراسة الوقائع النموذجية، كقضية "Cambridge Analytica"، وتطورات المعالجة الرقمية عربياً وأوروبياً.

خطة البحث **يتكون البحث من مبحثين رئيسيين:**

- **المبحث الأول** :الأطر القانونية لمعالجة البيانات الشخصية الرقمية
- المطلب الأول :الطبيعة القانونية للبيانات وضوابط معالجتها.
- المطلب الثاني :الإطار التشريعي المقارن لحماية البيانات الرقمية.
- **المبحث الثاني** :المسؤولية المدنية عن المعالجة غير المشروعة
- المطلب الأول :أركان المسؤولية (الخطأ – الضرر – العلاقة السببية).
- المطلب الثاني :صور المسؤولية وآليات التعويض، وتقييم للتشريعات المقارنة.

1. المبحث الأول

2. الإطار القانوني لمعالجة البيانات الشخصية الرقمية

شهد العصر الرقمي تطورًا نوعيًّا في مفهوم البيانات الشخصية، تجاوز فيه المعنى التقليدي للبيانات باعتبارها مجرد وسائط اتصال أو معلومات إدارية، إلى كونها عنصرًا مركزيًّا من عناصر الهوية القانونية للفرد. ومع دخول الذكاء الاصطناعي، والخوارزميات التنبؤية، وتقنيات التتبع المستمر في منظومات إدارة البيانات، أضحت عملية "المعالجة الرقمية "للبيانات نشاطًا قانونيًّا مستقلًا تتولد عنه آثار مدنية بالغة الخطورة، خاصة حينما يتم دون إذن، أو بمخالفة مبدأ الغرض المشروع، أو في ظل انعدام الشفافية.

وقد فرضت هذه التغيرات واقعًا قانونيًا جديدًا استدعى من التشريعات المعاصرة إعادة النظر في قواعد المسؤولية المدنية، فظهر في أوروبا، عبر اللائحة العامة لحماية البيانات(GDPR) ، نموذج متقدم لضبط المعالجة وتقييد سلطات المتحكم والمعالج بالبيانات. أما في الدول العربية، ورغم صدور تشريعات واعدة مثل القانون المصري رقم 151 لسنة 2020، فلا يزال العديد من الدول، وعلى رأسها العراق، يفتقر إلى تشريع خاص ينظم حماية البيانات بشكل صريح ومباشر.

ينطلق هذا المبحث من هذه الإشكالية ليعالجها من زاويتين مترابطتين: أولًا، **تحليل الطبيعة القانونية للبيانات الشخصية وضوابط معالجتها** بوصفها المدخل المفاهيمي والفني لفهم نطاق الحماية القانونية، وثانيًا، **بيان الأطر التشريعية المقارنة التي نظّمت هذه المعالجة**، واستجلاء مدى اكتمالها أو قصورها، في ضوء المعايير الدولية.

3. المطلب الأول

4. الطبيعة القانونية للبيانات الشخصية الرقمية وضوابط معالجتها

تأسيس المسؤولية المدنية عن الأضرار الناشئة عن معالجة البيانات الشخصية الرقمية يقتضي، قبل كل شيء، فهمًا دقيقًا **لماهية هذه البيانات وطبيعتها القانونية**، وما إذا كانت تُعامل في النظام القانوني كحق شخصي مستقل، أم أنها لا تزال في دائرة المعلومة أو الوسيلة. إذ إن تحديد الطبيعة القانونية

يُشكّل **الأساس المفاهيمي الذي تُبنى عليه الحماية القانونية من حيث المضمون والحدود.**

وعلاوة على ذلك، فإن معالجة هذه البيانات لا تنفصل عن الضوابط التي تُقيد مشروعيتها. فحتى إن قُبل التوصيف القانوني للبيانات على أنها حق، فإن الحماية المدنية لا تقوم إلا إذا ثبت تجاوز في حدود المعالجة. ومن هنا تظهر أهمية تحليل الضوابط الموضوعية والإجرائية التي تُنظم عمليات جمع البيانات، تخزينها، استخدامها أو نقلها.

لذلك، يعالج هذا المطلب في قسمه الأول **تعريف البيانات الشخصية الرقمية** بوصفها حقًا إنسانيًا وقانونيًا لصيقًا بالشخصية، ويُبيّن التمييز المفاهيمي والوظيفي بين **البيانات الشخصية العادية** وتلك ذات **الطابع الخاص أو الحساس،** قبل أن ينتقل إلى القسم الثاني لتحليل **ضوابط المعالجة القانونية المشروعة** في ضوء المبادئ العامة المستخلصة من التشريعات المقارنة، مع التوقف عند المفاهيم الجوهرية كالموافقة، والشفافية، وتحديد الغرض.

أولًا: تعريف البيانات الشخصية الرقمية كحق إنساني وقانوني: في خضم التوسع التقني غير المسبوق، لم تعد البيانات الشخصية مجرد أوصاف إدارية تُستخدم لأغراض إحصائية أو تنظيمية، بل غدت انعكاسًا مباشرًا للوجود القانوني للفرد، تتجلى فيها ملامح الهوية وتترتب على التعامل معها آثار قانونية جوهرية. وقد تحوّلت من كونها وسيلة إلى **محل حماية قانونية أصيلة،** على اعتبار أنها **حق غير مالي، لصيق بالشخصية، لا يقبل التصرف ولا السقوط بالتقادم** (Bygrave, 2014, p. 23; Desgens-Pasanau, 2015, p. 78).

وقد تبنّى النظام القانوني الدولي هذا المفهوم؛ إذ نصّت **المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان لعام 1950** على الحق في احترام الحياة الخاصة(Council of Europe, 1950) ، وتوسّع هذا الإقرار في **المادة 8 من ميثاق الحقوق الأساسية للاتحاد الأوروبي لعام 2000،** التي كرّست حماية البيانات الشخصية بوصفها حقًا مستقلاً، يخضع لضمانات مشددة، تشمل الشفافية، والموافقة، والرقابة (European Union, 2000; Fuster, 2014, pp. 120–123).

وفي السياق العربي، نص **الدستور المصري في المادة 57** على صيانة الحياة الخاصة، بما يشمل وسائل الاتصال، وحظر المساس بها إلا بأمر قضائي مسبب، وهو ما دعمته **المادة الأولى من القانون رقم 151 لسنة 2020،** التي عرّفت البيانات الشخصية وحددت ضوابط معالجتها القانونية، واشترطت وجود رضا صريح أو نص تشريعي (قانون حماية البيانات الشخصية المصري، 2020؛ محمود، 2024، ص. 1441).

وفي **القانون المغربي رقم 09.08،** تم تعريف المعطيات ذات الطابع الشخصي بأنها كل معلومة مرتبطة بشخص معرف أو قابل للتعرف عليه، وأخضعت معالجتها لرقابة اللجنة الوطنية لحماية المعطيات(CNDP) ، مع التزام بالشفافية والأمن المعلوماتي (المبطول، 2024، ص. 73–75). وقد اتفق الفقه المغربي المعاصر على أن حماية البيانات الرقمية تمثل صورة من صور صون الكرامة الإنسانية والحريات الشخصية.

أما في العراق، فعلى الرغم من غياب نص تشريعي صريح يُعرّف البيانات الشخصية الرقمية،

فقد نصت **المادة 1/43 من القانون المدني العراقي** على حماية الحياة الخاصة، وهو ما فُسّر فقهيًا بأنه يشمل البيانات الحديثة بوصفها امتدادًا قانونيًا للفرد، وأداة تمييز شخصي غير قابلة للتصرف (علي، 2023، ص. 231–233؛ الجبوري، 2011، ص. 92). ويُعد هذا القصور من أبرز أوجه الحاجة إلى إدماج البيانات ضمن الحقوق غير المالية المكفولة ذاتيًا.

ويُجمع الفقه العربي والغربي على أن البيانات الشخصية الرقمية باتت **حقًا موضوعيًا مستقلًا عن المصلحة المادية، لا تُعامل كمال ولا تُقوّم بثمن، بل تُحمى بذاتها**، أسوة بالجسد والصورة والكرامة، كونها تعكس جوهر الهوية القانونية للفرد (Desgens-Pasanau, 2015, p. 78; Hildebrandt, 2008, p. 34؛ العيش، 2023، ص. 290–291؛ سرور، 1975، ص. 114 .(وقد أشار العديد من الباحثين إلى أن هذا التطور في التكييف يفرض نظامًا قانونيًا خاصًا للمساءلة، يتجاوز قواعد الضرر التقليدية، ويرتكز على معيار "التحكم في البيانات" و"السيادة المعلوماتية للفرد (Bougeard, 2021, p. " 92).

وبذلك يتضح أن البيانات الشخصية الرقمية تُعد، في ضوء المقارنة التشريعية والتحليل الفقهي، **حقًا مدنيًا قائمًا بذاته، ضمن فئة الحريات الشخصية المحمية** .وأي انتهاك لها دون سند قانوني أو إذن صريح يُمثل اعتداءً على الكيان المعلوماتي للفرد، ويستوجب مساءلة مدنية مستقلة تُبنى على خصوصية الطبيعة الرقمية لا على مجرد مفاهيم الضرر المادي أو الإخلال بالتزام تقليدي. حيث أن البيانات الشخصية في شكلها الرقمي لم تعد مجرد وسيلة إجرائية، بل غدت **حقًا مستقلًا، ذا طبيعة غير مالية، يستحق حماية قانونية خاصة، توازي الحماية المقررة للكرامة والجسد والصورة والاسم** .(Desgens-Pasanau, 2015, p. 78;العيش، 2023، ص. 290–291؛ سرور، 1975، ص. 114.(وبناءً على ما تقدم يتضح لنا أن البيانات الشخصية الرقمية باتت وفقًا لهذا التوصيف المقارن تُعد **حقًا مدنيًا قائمًا بذاته،** لا يدخل في دائرة المال ولا المعاملات، بل في نطاق الحريات الشخصية ذات الطبيعة الخاصة. وبذلك فإن أي انتهاك لها دون إذن، أو على غير سند مشروع، يُشكّل اعتداءً على الكيان القانوني لصاحبها، ويستوجب تأسيس **مسؤولية مدنية خاصة** تخرج عن أحكام الضرر التقليدي، وتتطلب معايير جديدة قائمة على الخصوصية الرقمية، والحق في التحكم بالمعلومة الذاتية. وبالتالي، فإن الإطار القانوني المقارن يدفع باتجاه تكييف البيانات الشخصية الرقمية كحق مدني أصيل، يوجب الحماية الذاتية المستقلة، ويؤسس لبناء نظام مسؤولية مدنية منفصل، قائم على احترام الكيان المعلوماتي للفرد.

ثانيًا: التمييز بين البيانات الشخصية والبيانات ذات الطابع الخاص

: يُعد التمييز بين أنواع البيانات الشخصية من المسائل المحورية في بناء نظام قانوني فعال لحمايتها، إذ ليست جميع البيانات على نفس الدرجة من الخطورة أو التأثير على الكيان القانوني للشخص. وقد استقر الفقه المقارن على تقسيم البيانات إلى بيانات شخصية عادية، وأخرى ذات طابع خاص (حساس)، حيث تستدعي الأخيرة حمايات قانونية مضاعفة بسبب طبيعتها المرتبطة مباشرة بالكرامة الإنسانية، أو بسبب ما قد تُسببه من أضرار اجتماعية أو اقتصادية جسيمة في حال الإفشاء أو

المعالجة غير **المصرّح بها** (Bygrave, **2014, p. 95; Fuster, 2014, p. 126).**

ففي التشريع الأوروبي، تميز **المادة 4 من اللائحة العامة لحماية البيانات (GDPR)** بين البيانات الشخصية عامة، والتي تعني أي معلومة تتعلق بشخص معرف أو قابل للتعرف عليه، وبين البيانات ذات الطبيعة الخاصة كالعقيدة الدينية، أو المعتقدات السياسية، أو البيانات الصحية، أو الجينية، أو البيومترية، والتي يخضع جمعها ومعالجتها لقيود صارمة وفق المادة 9، ولا يجوز التعامل معها إلا في حالات استثنائية، وبموافقة صريحة ومستنيرة (GDPR, 2016/679, arts. 4–9).

ويكرّس **القانون المصري رقم 151 لسنة 2020** ذات المفهوم، حيث ميز في المادة 1 بند 8 بين "البيانات الشخصية" و"البيانات الشخصية الحساسة"، محددًا الأخيرة بأنها كل ما يتعلق بالحالة الصحية، أو الآراء السياسية، أو السمات الوراثية أو الجينية أو البيومترية، واشترط لمعاملتها إجراءات قانونية مشددة، تتمثل في الحصول على موافقة كتابية واضحة من صاحب البيانات، فضلًا عن شروط تتعلق بأمان التخزين والمعالجة (محمود، 2024، ص. 1442).

أما في **القانون المغربي رقم 09.08**، فقد حظرت المادة 1 معالجة بعض أنواع البيانات إلا بترخيص من اللجنة الوطنية، وبشروط خاصة، لا سيما إذا تعلق الأمر ببيانات الصحة أو الانتماء النقابي أو القناعات الشخصية أو الحياة الخاصة، معتبرة أن هذا الصنف يتمتع **بطبيعة قانونية مضاعفة الحماية** (المبطول، 2024، ص. 74–75).

وفي النظم الغربية، ولا سيما في فرنسا وألمانيا، تطور مفهوم البيانات ذات الطابع الخاص ليشمل كل ما يُمكّن من التمييز أو التصنيف بناءً على السمات غير الظاهرة للفرد، كالتحليل الجيني، أو الخصائص النفسية والسلوكية، ما فرض على الشركات والمؤسسات اتباع سياسات معالجة داخلية أكثر دقة (Desgens-Pasanau, 2015, p. 82).

أما **القانون المدني العراقي**، فإنه لا يتضمن نصًا صريحًا يُميّز بين هذه الفئات، حيث ترد حماية البيانات ضِمنًا في **المادة 1/43** المتعلقة بحماية الحياة الخاصة. وقد ذهب الفقه العراقي إلى أن هذا النقص التشريعي **يُضعف من الحماية المدنية للبيانات ذات الطابع الخاص**، ويجعلها عرضة للمعالجة دون معايير محددة، الأمر الذي يستوجب إدراج تفرقة تشريعية صريحة تستلهم التجارب المقارنة (علي، 2023، ص. 234؛ الجبوري، 2011، ص. 94).

وتأسيسًا على ما سبق، فإن التفرقة بين البيانات الشخصية العادية والبيانات ذات الطابع الخاص **ليست ترفًا مفاهيميًا بل ضرورة قانونية**، لأن الإخفاق في تمييزها يؤدي إلى تعارض في درجات الحماية، وغموض في المسؤولية المدنية، فضلًا عن أنه يُجهض مبدأ التناسب بين طبيعة البيانات والإجراءات القانونية المقررة لمعالجتها.

المطلب الثاني

الإطار القانوني لحماية البيانات الشخصية الرقمية

إذا كانت المعالجة السابقة قد تناولت الطبيعة القانونية للبيانات الشخصية الرقمية وضوابط التعامل معها بوصفها حقًا إنسانيًا لصيقًا بالشخصية القانونية، فإن ما يترتب على هذا التوصيف من آثار لا يكتمل إلا عبر الوقوف على الإطار القانوني المنظِّم لتلك المعالجة. ذلك أن الحماية القانونية لا تقوم فقط على إثبات الحق، بل تتطلب **بنية تشريعية واضحة تُحدِّد الضوابط والمسؤوليات والجزاءات** عند الاعتداء على هذا الحق.

وفي ظل تعاظم التهديدات الرقمية وتعدد صور الانتهاك للمجال المعلوماتي للأفراد، برزت الحاجة إلى **تشريعات خاصة تُعنى بحماية البيانات الشخصية** تنظيميًا ومدنيًا، وهو ما سعت إليه بعض الدول في أنظمتها الحديثة، بينما لا تزال أنظمة أخرى تفتقر إلى التنظيم التفصيلي، مكتفية بالإحالة إلى مفاهيم عامة كحماية الخصوصية أو الحياة الخاصة.ومن هنا، فإن هذا المطلب يُعنى بتحليل **الإطار القانوني الحاكم لمعالجة البيانات الشخصية الرقمية**، وذلك على التفصيل التالي:

أولًا: التشريعات الدولية والمحلية المنظمة لمعالجة البيانات : لقد فرضت الثورة الرقمية واقعًا تشريعيًا جديدًا، أصبح معه من الضروري وضع أنظمة قانونية متخصصة تنظم عمليات جمع ومعالجة البيانات الشخصية. ولم يعد الاكتفاء بالإحالة إلى قواعد المسؤولية العامة كافيًا، بل تطلب الأمر **تبني تشريعات مستقلة تُعنى بتحديد نطاق المعالجة، وضمانات الحماية، وآليات الرقابة والمساءلة**، بما يضمن التوازن بين حق الأفراد في الخصوصية واحتياجات المجتمع الرقمي.

التشريع الأوروبي: اللائحة العامة لحماية البيانات (GDPR):تُعد **اللائحة العامة لحماية البيانات الأوروبية (GDPR)**الصادرة بموجب **تنظيم الاتحاد الأوروبي رقم 679/2016** نقطة تحول رئيسية في تاريخ حماية البيانات، إذ أضفت على البيانات الشخصية صفة الحق الأساسي، وفرضت التزامات صارمة على المعالِجين والمتحكمين في البيانات. وقد عرّفت المادة 4 منها البيانات الشخصية بأنها "كل معلومة تتعلق بشخص طبيعي معرف أو يمكن التعرف عليه"، ثم نظّمت المواد 5 إلى 11 مجموعة من المبادئ الحاكمة كالموافقة، والحد من الغرض، والدقة، والمساءلة.(European Union, 2016)

ويُعد هذا التنظيم من أكثر الأطر القانونية تفصيلًا وتقييدًا، حيث يُلزم المشغّلين بالحصول على إذن مسبق، وتقديم معلومات واضحة، وضمان أمن البيانات، مع رقابة فعالة من سلطات مستقلة، فضلًا عن وضعه لغرامات تصل إلى 4% من الإيرادات السنوية العالمية للجهة المخالِفة، ما جعله مرجعًا عالميًا للتشريعات اللاحقة (Bygrave, 2014, pp. 63–65).

●التشريع المصري: القانون رقم 151 لسنة 2020 أما في مصر، فقد تم إصدار **القانون رقم 151 لسنة 2020 بشأن حماية البيانات الشخصية**، والذي يُعد خطوة متقدمة في سياق التنظيم العربي. وقد نصت مادته الأولى على تعريف شامل للبيانات الشخصية، وتفريق واضح بين البيانات العادية وتلك ذات الطابع الحساس، كما ألزم في المواد (2–7) بالحصول على **موافقة صريحة مسبقة** من صاحب البيانات، وفرض قيودًا على الإفصاح أو المعالجة لأغراض غير محددة سلفًا.

ويتميز القانون المصري بتأسيس **مركز حماية البيانات الشخصية**، كهيئة مستقلة تختص بإصدار التراخيص، وضبط آليات الامتثال، وتلقي الشكاوى، وهو ما يعكس إدراكًا تشـــريعيًا متقدمًا بأهمية البنية المؤسسية للحماية (محمود، 2024، ص. 1443؛ القانون 151 لسنة 2020، م2–م6).

●التشريع المغربي: القانون رقم 09.08 وفي المغرب، جاء **القانون رقم 09.08** الصـــادر ســـنة 2009 ليؤســـس لنظام متقدم نســـبيًا في البيئة المغاربية، حيث نظم حماية المعطيات الشـــخصـــية على نحو دقيق، مع الإلزام بـالإخطـار، والموافقـة، والتســـجيل المســـبق للمعالجة، خاصـــة إذا تعلقت ببيانات حســاســة أو بعمليات نقل دولية للمعلومات. وقد تم تأســـيس **اللجنة الوطنية لحماية المعطيات (CNDP)**كجهة رقابية ذات صـــلاحيات واســـعة (المبطول، 2024، ص. 72–75).

ورغم الريادة النســـبية للتجربة المغربية، إلا أن التطبيق العملي ظل دون المستوى المطلوب، بسبب محدودية الإمكانات الرقابية، وغياب ثقافة الامتثال الرقمي في القطاعين العام والخاص.

●*التجربة العراقية: غياب التنظيم التشريعي الخاص* أما في العراق، فلا يوجد حتى الآن قانون خاص لحماية البيانات الشخصية، رغم تزايد الدعوات الفقهية لتبنّيه. ويُلاحظ أن **المادة 43 من القانون المدني العراقي** تُقر حماية الحياة الخاصة، إلا أنها **لا تكفي لتأسيس تنظيم دقيق لعمليات المعالجة**، خاصة مع غياب جهة رقابية مختصة أو آلية واضحة للترخيص أو المراقبة (علي، 2023، ص. 235). وقد أشار الفقه العراقي إلى أن **الفراغ التشريعي يشكل عائقًا أمام مساءلة الجهات التي تُخزّن أو تعالج البيانات دون إذن أو بمخالفة لمبادئ الحماية الحديثة.**

●*التجارب العربية الأخرى* يجدر الإشارة إلى أن دولًا عربية أخرى تبنت تشريعات حديثة نسبيًا، مثل **قانون حماية البيانات السعودي لسنة 2021**، **ومشروع القانون التونسي** المقترح في 2023، وكلاهما يستلهم مبادئ GDPR، لا سيما في ما يتعلق بالموافقة، وتقييد الغرض، وحظر النقل خارج الحدود بدون ضمانات تعاقدية. ومع ذلك، فإن **ضعف التطبيق، أو غياب الهيئات الرقابية المستقلة، ما يزال يمثل تحديًا في النظم العربية.**

يتضح من العرض المقارن أن التنظيم القانوني لحماية البيانات يراوح بين **نموذج متقدم (الاتحاد الأوروبي)، ونموذج ناشـــئ في تطور (مصـــر، المغرب، الســعودية)، وفراغ تشـريعي تام (العراق)**، ما يؤكد الحاجة الماســـة إلى **بناء منظومة وطنية عراقيـة تســـتلهم النمـاذج الـدوليـة، مع مراعـاة الخصوصية الاجتماعية والقانونية العراقية.**

ثانيًا: التزامات الجهات المعالجة للبيانات: لا تكتمل الحماية القانونية للبيانات الشخصية الرقمية إلا بتحديد واضح وصارم للالتزامات التي تقع على عاتق "الجهات المعالجة"، سواء أكانت جهة متحكمة في البيانات (Controller) أو جهة تقوم على معالجتها لحساب الغير .(Processor) وهذه الالتزامات لا تُعد تنظيمية فحسب، بل تشكّل جوهر المسؤولية القانونية إذا ما أُخِلّ بها، وهو ما يجعلها ركيزة في بناء النظام القانوني للحماية الرقمية.

ويُجمع التشريع المقارن على أن هذه الالتزامات **تنقسم إلى محورين متكاملين :**محور إجرائي يتعلّق بالإعلام، والشفافية، والموافقة، ومحور تقني يتصل بتأمين البيانات وتسجيل المعالجات والالتزام بالإخطار حال الانتهاك.

.1الالتزامات الإجرائية: نصّ الـــ **GDPR** الأوروبي في مواده من 12 إلى 23 على **حق صـاحب البيانات في الحصـول على المعلومات قبل المعالجـة، ووجوب موافقتـه الصـــريحـة، وحقه في**

الاطلاع والتعديل والمحو، بل والاعتراض على المعالجة، وأوجب على المعالج توفير إشعار خصوصية يحدد بوضوح أغراض المعالجة والجهات التي يُفصح لها (European Union, 2016, arts. 12–23).

وفي مصر، ألزم القانون رقم 151 لسنة 2020 المسؤول عن المعالجة بتوفير بيانات دقيقة لصاحب البيانات، وتسجيل جميع عمليات المعالجة، وإخطاره حال حدوث اختراق أو إفصاح غير مشروع، فضلًا عن وجوب الحصول على موافقته المسبقة، إلا في حالات استثنائية حددها القانون على سبيل الحصر (قانون حماية البيانات المصري، م4، م7، م10)حماية البيانات الشخصية....

أما في المغرب، فإن القانون رقم 09.08 فرض على المسؤول عن المعالجة ضرورة التصريح المسبق لدى اللجنة الوطنية لحماية المعطيات (CNDP)، مع إلزامه بالإعلام المسبق للمعنيين، وتقييد الإفصاح والغرض، وعدم جمع سوى البيانات الضرورية (قانون رقم 09.08، مادة 5–7)مغربي المسؤولية المدنية....

.2الالتزامات الفنية: يُعد البعد الفني أحد أعمدة الحماية، حيث يُفرض على الجهات المعالجة الالتزام بوسائل تقنية "فعّالة ومتناسبة" مع حساسية البيانات. وقد بيّنت الـ GDPRذلك صراحة في المادة 32، التي أوجبت تشفير البيانات، إدارة الوصول، تقييم الأثر المسبق، ووضع خطط استجابة للحوادث، وهو ما يرسّخ مفهوم "المساءلة الوقائية preventive) " (accountabilityحماية البيانات الشخصية....

وفي التشريع المصري، نصت المادة (8) من القانون على إلزام المعالج باتخاذ جميع التدابير الفنية والإدارية الكفيلة بتأمين البيانات، ووضع السياسات اللازمة لمنع الاختراق والاختلاس، وهو ما تدعمه اللائحة التنفيذية بتحديد معايير الأمان (محمود، 2024، ص. 1452)حماية البيانات الشخصية....

بينما ألزم القانون المغربي كل جهة معالجة بأن تحفظ سرية المعطيات الشخصية، وتُخضع موظفيها لواجب الكتمان، ولو بعد انتهاء عملهم، وهو التزام يصل إلى مرتبة الجزاء الجنائي في حال الإخلال (قانون 09.08، مادة 24–27)مغربي المسؤولية المدنية....

.3المضمون المقارن وتوصيف الخلل العراقي:

يتضح من المقارنة أن معظم التشريعات المتقدمة **تبني نظامًا دقيقًا للامتثال الإداري والفني**، وتربط بين الإخلال بهذه الالتزامات وبين نشوء المسؤولية المدنية. أما في العراق، فلا تزال هذه الالتزامات غير منصوص عليها تشريعيًا، بل تُستمد استنادًا إلى التكييف الفقهي للالتزام العام بعدم الإضرار، مما يجعل إثبات الخطأ أمرًا شاقًا في القضايا الرقمية، ويُضعف من فعالية الحماية (الجبوري، 2011، ص. 92؛ علي، 2023، ص. 238)حماية البيانات الشخصية....

ومن وجهة نظرنا لم تعد الالتزامات الواقعة على الجهة المعالجة مجرد واجبات تنظيمية، بل غدت أساسًا حاسمًا في تحديد مدى شرعية المعالجة من عدمها، وتُشكّل، حال الإخلال بها، سببًا مباشرًا لنشوء المسؤولية المدنية. ولهذا، فإن تطوير الإطار العراقي يتطلب دمج هذه الالتزامات بشكل صريح، واستلهام النموذج الأوروبي في توزيع المسؤوليات وتبني آليات رقابية قائمة على معايير الامتثال الشامل.

وأخيراً ومن خلال استعراضنا المتقدم للالتزامات الإجرائية والفنية الواقعة على الجهات المعالجة للبيانات يتبيّن أن هذه الالتزامات ليست مجرد أدوات تنظيمية لحسن إدارة البيانات، بل تمثل في جوهرها أساسًا موضوعيًا للمساءلة القانونية عند الإخلال بها .فكل تقصير في الحصول على الموافقة، أو في توفير الشفافية، أو في تأمين البيانات على نحو ملائم، لا يُعد مخالفة إدارية فحسب، بل يرتقي إلى مصاف الخطأ المدني متى ترتب عليه ضرر فعلي أو محقق لصاحب البيانات، وعليه، فإن البناء القانوني لحماية البيانات الشخصية الرقمية لا يكتمل دون تحديد دقيق لمسؤولية الجهة المعالجة حال الإخلال بالتزاماتها، سواء في إطار العلاقة التعاقدية أو على أساس الخطأ التقصيري. وتُعد هذه النقطة مدخلًا لازمًا للانتقال إلى المبحث الثاني من هذا البحث، والذي يتناول تفصيلًا شروط وأركان وآثار المسؤولية المدنية الناتجة عن انتهاك معالجة البيانات الشخصية الرقمية، بما في ذلك تحديد طبيعة الخطأ، وتمييز أنواع الضرر، والعلاقة السببية بين الإخلال والنتيجة.

المبحث الثاني

المسؤولية المدنية الناتجة عن انتهاك معالجة البيانات الشخصية الرقمية

أثبت التحليل السابق أن حماية البيانات الشخصية الرقمية لا تقتصر على إنشاء التزامات تنظيمية وفنية، بل تتطلب بالضرورة **نظامًا قانونيًا للمساءلة يضبط جزاء الإخلال بتلك الالتزامات** . فالمعالجة غير المشروعة للبيانات، سواء وقعت بدون إذن، أو تجاوزت الغرض المشروع، أو تمت بإهمال في وسائل الحماية، تؤدي إلى إلحاق أضرار بالغة بصاحب البيانات، وتُثير التساؤل الجوهري حول **كيفية تنظيم المسؤولية المدنية في مواجهة هذا الانتهاك.**

وفي ظل الطبيعة الخاصة للبيانات الرقمية – كونها غير مادية، قابلة للنسخ والانتشار، ويتعذر في الغالب حصر أثر انتهاكها ماديًا – ظهرت **حاجة ملحة لإعادة صياغة المفاهيم المدنية التقليدية،** لا سيما أركان المسؤولية الثلاثة: الخطأ، والضرر ،والعلاقة السببية. كما تطلب الأمر **تمييزًا بين صور المسؤولية العقدية، متى وُجد التزام سابق، والمسؤولية التقصيرية عند غياب رابطة تعاقدية،** مع بيان أثر نقل عبء الإثبات في القضايا الرقمية. وسيعالج هذا المبحث هذه الإشكاليات من خلال المطلبين التاليين:

المطلب الأول

أركان المسؤولية المدنية عن انتهاك معالجة البيانات الشخصية

تُعد المسؤولية المدنية عن انتهاك البيانات الشخصية الرقمية في جوهرها انعكاسًا لانتقال مركز الثقل من الحماية الإجرائية إلى الحماية الموضوعية، حيث لم يعد كافيًا – في ظل الانفجار المعلوماتي – الاكتفاء بوضع ضوابط تنظيمية للمعالجة، بل بات من اللازم إحاطة هذا النظام بضمانات قضائية، تُمكّن المتضرر من الحصول على جبر حقيقي للضرر، متى ثبت الإخلال.وبينما ويُعتبر تحليل أركان هذه المسؤولية – وتحديدًا الخطأ والضرر والعلاقة السببية – محورًا تأسيسيًّا لفهم كيف تتفاعل القواعد المدنية مع الخصوصيات الرقمية، خاصة في ظل اتساع نطاق المعالجة، وارتباطها بتقنيات معقدة

كالتعلم الآلي، والتجميع التلقائي للبيانات، والاستهداف الإعلاني الدقيق. كما يطرح هذا التحليل تساؤلات جوهرية حول ما إذا كانت القواعد التقليدية للمسؤولية لا تزال قادرة على احتواء هذه الانتهاكات، أم أن الأمر يقتضي إعادة بناء نظرية الخطأ المدني على أسس جديدة تتلاءم مع الواقع الرقمي المتحوّل. من هذا المنطلق، يعالج هذا المطلب – بأسلوب مقارن وتحليلي – كيفية تكوّن المسؤولية المدنية في حالات انتهاك المعالجة، مع بيان كيف فسّرت النظم القانونية المختلفة هذه الأركان، وكيف تعامل الفقه والقضاء مع التحديات العملية والإثباتية التي يثيرها الانتهاك الرقمي. وينقسم هذا المطلب إلى العنصرين الأساسيين التالي بيانهما:

أولًا: الخطأ كركن أساسي في المسؤولية المدنية عن المعالجة غير المشروعة للبيانات: يشكل الخطأ الركن المحوري في بناء المسؤولية المدنية التقليدية، سواء في صورتها العقدية أو التقصيرية، ويُفهم عمومًا على أنه إخلال بالتزام قانوني أو سلوك منحرف عن السلوك المتوقع من الشخص المعتاد، سواء بالفعل أو الامتناع، متى أدى ذلك إلى الإضرار بالغير. وقد شهد هذا المفهوم تحولًا نوعيًا في البيئة الرقمية، حيث بات الخطأ يشمل صورًا غير تقليدية ترتبط بالإخلال بالمبادئ المعلوماتية الجوهرية، مثل الشفافية، والموافقة الحرة، وتحديد الغرض، وتدابير الأمان، ما يفرض إعادة ضبط لمفاهيم الخطأ في ضوء الخصوصيات التقنية المعاصرة.

في هذا السياق، تُعد المعالجة غير المشروعة للبيانات، أو تلك التي تتم دون سند قانوني أو بالمخالفة للغرض المعلن، صورة نموذجية للخطأ في القانون الأوروبي، حيث اعتبرت المادة 82 من اللائحة العامة لحماية البيانات (GDPR) أن كل انتهاك لأحكامها يوجب المسؤولية، ما لم يثبت المعالج أو المتحكم أنه لم يكن مسؤولًا عن الفعل الضار (European Union, 2016, art. 82). ويُستدل من ذلك أن الخطأ في هذا النطاق يُفترض بمجرد حدوث المعالجة المخالفة، دون اشتراط إثبات القصد أو الإهمال، وهو ما يشكّل تحولًا بنيويًا من المسؤولية القائمة على الإثبات إلى المسؤولية القائمة على الخطأ المفترض أو الموضوعي.

وفي مصر، رسخ القانون رقم 151 لسنة 2020 ذات الاتجاه، حيث نصت المادة الرابعة منه على التزامات صارمة على المعالجين، وألزمتهم بالحصول على موافقة صريحة ومحددة من صاحب البيانات قبل البدء في المعالجة، كما اعتبرت المعالجة دون سند قانوني أو خارج الإطار المعلن إخلالًا يوجب الجزاء والتعويض، دون أن يتطلب النص ثبوت الخطأ كشرط مستقل (قانون حماية البيانات الشخصية المصري، 2020، م4).

أما في المغرب، فرغم أن الفصل 78 من قانون الالتزامات والعقود يقوم على المسؤولية المبنية على إثبات الخطأ، إلا أن القانون رقم 09.08 المتعلق بحماية المعطيات ذات الطابع الشخصي يشير إلى فرض التزامات وقائية مسبقة على المعالج، مثل التصريح المسبق والإخطار، ما يعني أن مجرد الإخلال بها يُعد خطأ مفترضًا يوجب التعويض، كما استقر عليه القضاء المغربي في عدد من أحكامه (قانون 09.08، م12، م18).

وفي العراق، ورغم عدم وجود تشريع خاص بحماية البيانات الشخصية حتى الآن، إلا أن الفقه اتجه إلى تكييف المعالجة غير المشروعة ضمن

إطار المسؤولية التقصيرية في القانون المدني، لا سيما المادة 204، التي تعتبر كل فعل يُحدث ضررًا بالغير خطأً موجِبًا للتعويض، ما يسمح بتطبيق نظرية الخطأ المفترض في حال ثبتت المعالجة المخالفة وانعدمت وسائل الإثبات لدى الضحية.

تعددت صور الخطأ في البيئة الرقمية، من أبرزها: المعالجة دون موافقة صريحة، والإفشاء غير المصرح به، والإهمال في التأمين الإلكتروني للبيانات، واستخدام البيانات في غير الغرض المعلن، ورفض الاستجابة لطلبات التصحيح أو الحذف. وقد عكست هذه الصور أن الخطأ لم يعد مقصورًا على الفعل المادي، بل امتد ليشمل القرارات الإدارية، والإغفال التقني، والسلوك السلبي في الالتزام بضوابط الحماية.

وقد كرّست التطبيقات القضائية الدولية هذا التوجه. فقد اعتبرت محكمة العدل الأوروبية في قضية Google Spain v. AEPDأن مجرد الاحتفاظ بنتائج بحث تتضمن معلومات ضارة، رغم انعدام الغرض منها، يُعد خطأ يُرتب مسؤولية الشركة عن الضرر المعنوي الواقع بالمستخدم (CJEU, 2014, Case C-131/12).وفي واقعة Cambridge Analytica، أدانت لجنة التجارة الفيدرالية (FTC) شركة فيسبوك بسبب استخدام بيانات المستخدمين دون علمهم، وفرضت غرامة تاريخية تجاوزت خمسة مليارات دولار، ما يعكس تبني النظام الأمريكي للمسؤولية شبه الموضوعية في قضايا المعالجة الرقمية.(FTC, 2019)

وفي فرنسا، أصدرت CNIL قرارًا بتغريم شركة Googleلعدم وضوح سياستها بشأن جمع البيانات، رغم عدم وجود دليل على وقوع ضرر مباشر، مما يؤكد اعتماد الخطأ المفترض كأساس تنظيمي للحماية .(CNIL, 2019) كما حكمت محكمة في الرباط الابتدائية على جهة إعلامية بالتعويض لصالح موظفة تم استخدام اسمها في موقع إلكتروني دون إذن، بعد انتهاء علاقتها بالمؤسسة، وعدّت ذلك إفشاءً غير مشروع يعكس صورة من صور الخطأ القانوني.

يتضح من التحليل أن الخطأ في المعالجة الرقمية بات يُفترض بمجرد مخالفة الإطار القانوني المنظم للبيانات، وأن اتجاه المشرّع المقارن يميل إلى إعلاء مبدأ الاحتياط والوقاية، لا سيما في ظل اختلال مراكز القوة بين المعالج وصاحب البيانات. وهو ما يُبرر الانتقال من نموذج "الخطأ الواجب الإثبات" إلى نموذج "الخطأ المفترض"، الذي يحقق حماية فعالة للحق في الخصوصية الرقمية، ويؤسس لمسؤولية مدنية تتلاءم مع طبيعة الفضاء المعلوماتي. فباستجلاء مضمون الخطأ في إطار المعالجة الرقمية للبيانات يكشف عن تحوُّل عميق في المفهوم الكلاسيكي للمسؤولية المدنية، لم يعد مقتصرًا على معيار السلوك المعتاد أو فكرة الإهمال المادي، بل تجاوزه إلى نطاق من الضوابط المعلوماتية التنظيمية، تشكل كل منها التزامًا قانونيًا قائمًا بذاته، يُعد الإخلال به قرينة قائمة على الخطأ لا تقبل التهوين. فالخطأ، وفق المنظور الرقمي المعاصر، لم يعد فعلاً ضارًا فقط، بل أصبح انتهاكًا للنسق القانوني الحاكم لشرعية المعالجة، بدءًا من الموافقة، ومرورًا بالغرض، وانتهاءً بتأمين البيانات وإتاحة التحكم لصاحبها (Bygrave, 2014, pp. 52–59; Fuster, 2014, pp. 120–123).

وقد تأكد ذلك الاتجاه في أحدث اجتهادات القضاء المقارن. فقد قررت محكمة النقض المغربية في حكمها الصادر عام 2022 ضد جريدة "مساء

ميديا" أن عدم تحديث بيانات موظف سابق يمثل إخلالًا بالمعالجة الواجبة قانونًا، مما أوجب التعويض رغم انعدام الضرر المالي المباشر (مغربي، 2024، ص. 148). وذهبت محكمة العدل الأوروبية في حكمها لعام 2023 إلى إدانة شركة سويدية أجرت معالجة بلا تحديد مسبق للغرض، واعتبرت هذا التصرف كافيًا بذاته لقيام الخطأ، دون حاجة لإثبات النية أو الضرر (Court of Justice of the European Union, 2023). بل إن المحكمة العليا البريطانية في قضية Lloyd v. Google LLC قررت أن مجرد استخدام بيانات المتصفح دون علم المستخدم يُكوِّن خطأً مدنيًا مستقلًا، ترتب عليه مسؤولية تقصيرية قائمة، حتى في غياب عقد أو ضرر مادي.(UKSC, 2021/0175)

كما أصدرت اللجنة الوطنية الفرنسية للمعلومات والحريات (CNIL) في 2022 قرارًا ضد شركة Clearview AI ، قضت فيه بأن استخدام البيانات البيومترية علنًا من الإنترنت دون موافقة يشكل خرقًا جسيمًا لضوابط المعالجة، ما استتبع فرض غرامة قدرها 20 مليون يورو (CNIL, 2022).

تُبرز هذه الأحكام مجتمعة أن معيار الخطأ في البيئة الرقمية أصبح معيارًا موضوعيًا في جوهره، ومفترضًا في آثاره، يتأسس على مجرد الإخلال بالمقتضيات الفنية أو التنظيمية التي أقرها المشرّع. ومع ذلك، تبقى بعض التشريعات، وعلى رأسها النظام القانوني العراقي، قاصرة عن مواكبة هذا التطور، حيث ما زالت تتعامل مع المعالجة الرقمية بمنظور تقليدي، لا يتيح للمتضرر سوى اللجوء إلى القواعد العامة في إثبات الخطأ، ما يُضعف الحماية المدنية في مواجهة الانتهاك المعلوماتي (الجبوري، 2023، ص. 92–96).

وعليه، فإن التحليل المقارن لم يعد فقط كاشفًا عن تفاوت الحماية، بل أصبح دافعًا لإعادة بناء المفاهيم المدنية حول الخطأ، بصورة تُدرج المعالجة غير المشروعة للبيانات ضمن الوقائع المدنية المولِّدة لمسؤولية خاصة، قائمة على افتراض الخطأ في ذات الفعل لا في النية، ومقتضية لنظام إثبات عكسي، يحمّل المعالج عبء نفي مسؤوليته لا العكس (Fuster, 2014, pp. 123–126; European Union, 2016, Art. 82).

5. ***ثانيًا:*** الضرر كركن في المسؤولية المدنية عن المعالجة غير المشروعة للبيانات الشخصية الرقمية

أضحى الضرر في نطاق المعالجة الرقمية للبيانات الشخصية مفهوماً متطوّرًا يتجاوز الأطر التقليدية للتعويض المدني. فبينما كان يشترط في الفقه المدني الكلاسيكي أن يكون الضرر ماديًا، محققًا، ومباشرًا، فإن التطورات القضائية والتشريعية في العصر الرقمي قد فرضت إعادة تشكيل هذا الركن ليشمل صورًا جديدة من الأذى، وفي مقدمتها الضرر الأدبي، النفسي، والاحتمالي.

ولقد أرست اللائحة العامة لحماية البيانات في الاتحاد الأوروبي(GDPR) ، لا سيما في المادة 82، مبدأً حاسمًا مفاده أن أي شخص لحقه "ضرر مادي أو معنوي" نتيجة خرق لأحكامها، يستحق تعويضًا عادلًا. وقد تبنّت محكمة العدل الأوروبية هذا الاتجاه، مُعتبرة أن مجرد فقدان السيطرة على البيانات الشخصية يعد ضررًا قائمًا بذاته، لا يحتاج إلى إثبات مباشر للضرر المالي أو المادي (European Union, 2016, Art. 82).

وفي هذا السياق، توسّعت النظم الأوروبية في تفسير الضرر الرقمي:

- فقد أقرت محكمة دوسلدورف الإقليمية بألمانيا سنة 2023 بتعويض قدره 5,000 يورو عن تسريب بيانات طبية، رغم عدم تحقق ضرر مالي مباشر، مستندة إلى التهديد المعنوي الذي لحق بالمدعي.(Az. 12 O 267/22)
- وأكدت محكمة ميلانو سنة 2022 أن نشر بيانات حساسة على وسائل التواصل يمثل ضررًا نفسيًا ومعنويًا يستوجب التعويض حتى دون تحقق أثر اقتصادي، وألزمت الجهة المخالفة بتعويض قدره 15,000 يورو.(RG n. 11775/2022)
- وفي **هولندا**، قضت محكمة أمستردام سنة 2024 بتعويض موظفة عن انتهاك هويتها المعلوماتية داخل تقارير داخلية، رغم عدم ثبوت تشهير علني، واعتبرت ذلك ضررًا معنويًا مهنيًا بالغ الخطورة.
- أما في **إسبانيا**، فقد قُدّرت التعويضات في قضية رقم PS/00042/2023 بقيمة 2,500 يورو لكل فرد، عن تسريب أرقام هواتف وبريد إلكتروني، مؤكدين أن تقييم الضرر المعنوي يجب أن يُراعى فيه شدة الانتهاك ومدته ونطاق انتشاره.

وفي الدول العربية، تباين الموقف:

- ففي **مصر**، أقر قانون حماية البيانات الشخصية رقم 151 لسنة 2020 بالتعويض عن الضرر الأدبي دون اشتراط ماديته، وهو ما انسجم مع أحكام النقض المصري التي قررت تعويضًا في حالات إفشاء البيانات دون إذن (قانون حماية البيانات الشخصية المصري، 2020؛ محمود، 2024، ص. 1457).

أما **في العراق**، فرغم غياب قانون خاص، فإن المادة 202 من القانون المدني تُجيز التعويض عن الضرر غير المالي، وقد فُسّرت فقهيًا على نحو يتيح إدراج الأذى المعلوماتي أو الأدبي ضمن الضرر المدني القابل للتعويض (الجبوري، 2023، ص. 95).

تُجمع هذه الأنظمة على أن الضرر في البيئة الرقمية قد يتجلى بصور غير تقليدية، من أبرزها:

- فقدان التحكم بالبيانات.
- القلق النفسي الناتج عن علم الشخص أن بياناته عرضة للاختراق.
- إساءة استخدام المعطيات دون أن يتم تداولها علنًا.
- التصنيف الخوارزمي المؤدي إلى تمييز مهني أو اجتماعي.

ولذلك، فإن الضرر الرقمي لا يُشترط فيه المادية أو القابلية للقياس الكمي، بل يُعتد فيه بصفته انتهاكًا شخصيًا ذاتيًا، يرتب التزامًا بالتعويض في ضوء مبدأ حماية الكيان المعلوماتي للفرد.

ونرى من وجهة نظرنا أن الضرر لا يقف في مجال المعالجة الرقمية للبيانات عند حدود الانتهاك الظاهر أو الأثر المباشر، بل يُمثل نقطة تقاطع جوهرية بين الحق الشخصي في الهوية المعلوماتية، والواجب القانوني في صون المجال الخاص للفرد من الاختراق أو التلاعب. وقد بات واضحًا أن المعالجة غير المشروعة لا تُقاس خطورتها فقط بنتيجتها، بل بطبيعتها الذاتية وما تحمله من إمكانات الإضرار لاحقًا، وهو ما يفرض إعادة تشكيل مفهوم الضرر نفسه، قانونيًا وقضائيًا. ففي عصر تتداخل فيه الخوارزميات مع الحياة اليومية، أضحى مجرد الاحتفاظ غير المصرح به بالمعلومة، أو استخدام نظام تحليل بيانات يُقصي فردًا أو يصنفه دون علمه، فعلاً مضرًا يستحق التعويض، ولو لم يُفضِ إلى

خسارة مالية أو سمعة مباشرة. ذلك أن القيمة المركزية اليوم لم تعد المال، بل التحكم بالبيانات، باعتباره جوهر الكيان القانوني الحديث للفرد. وما يلفت في الاجتهاد الأوروبي، أن تطور مفهوم الضرر جاء ليس فقط عبر المحاكم، بل في بنية النصوص التشريعية ذاتها، حيث وُضع الضرر المعنوي في صدارة المفاهيم القابلة للتعويض(GDPR, Art. 82) ، وأصبح يُنظر إلى المعالجة المنحرفة كفعل منشئ للمسؤولية، دون الحاجة إلى ترسيخ قواعد إثبات تقليدية. فهذه النزعة المتقدمة تُحتم على النظم العربية، ولا سيما التشريع العراقي، أن تُعيد النظر في مركزية الضرر المالي ضمن أحكام المسؤولية المدنية. فالمعالجة الرقمية التي تُنتج قلقًا دائمًا، أو تنتهك الشعور بالأمان المعلوماتي، أو تُنتج تصنيفًا خفيًا يقيّد فرص الفرد في العمل أو التمويل، هي ضرر مدني كامل الأركان، وإن اتخذ شكلاً غير تقليدي. ومن هنا، يجب أن يتطور مفهوم "الضرر" في الفقه المدني، ليشمل الانتهاك غير الظاهر، والضرر الاحتمالي المؤسَّس على خرق الحقوق الرقمية، وحرمان الفرد من تقرير مصيره المعلوماتي .وهذا لا يتحقق إلا بإدماج معيار "المساس بالحق في السيطرة على البيانات" ضمن مفاهيم الضرر الموجبة للمسؤولية، وفتح الباب أمام تطوير قواعد الإثبات، لتُراعي طبيعة المعالجة الرقمية، وما تستبطنه من أثر صامت ممتد. ولعل ذلك يُشكّل اللبنة الأساس لبناء نظرية حديثة في المسؤولية المدنية الرقمية، تُعيد الاعتبار للكرامة الرقمية كعنصر غير قابل للتفريط أو التبعيض.

6. المطلب الثاني

7. العلاقة السببية وصور المسؤولية المدنية في معالجة البيانات الشخصية الرقمية

في ظل التحول الرقمي المتسارع وما يصاحبه من استحداث آليات جديدة لمعالجة البيانات الشخصية، لم تعد أنماط المسؤولية المدنية خاضعة للمفاهيم الكلاسيكية فقط، بل باتت تستوجب معالجة قانونية أكثر مرونة تتناسب مع طبيعة البيئة الرقمية التي تطرح إشكاليات فريدة في نطاق العلاقة بين الخطأ والضرر. ولعل من أبرز هذه الإشكاليات ما يتعلق بإثبات **العلاقة السببية** في إطار المعالجة الرقمية، حيث غالبًا ما تتداخل الأفعال التقنية لعدة أطراف، ويصعب تحديد الفاعل المباشر للضرر أو التمييز بين المراحل التي وقعت فيها المعالجة غير المشروعة، مما يُصعّب من عبء الإثبات على المتضرر. ومن جانب آخر، تفرض التعددية في صور الانتهاك الرقمي – بين إفشاء غير مصرح به، أو تخزين بلا إذن، أو معالجة تفتقر للشفافية – ضرورة تفكيك أنماط المسؤولية المدنية التي قد تنشأ: بين مسؤولية عقدية تستند إلى إخلال بالتزامات حماية البيانات المقررة في العقود الإلكترونية، ومسؤولية تقصيرية تُبنى على الإخلال بواجبات الحيطة والحذر المفروضة قانونًا ولو في غياب العلاقة التعاقدية. وانطلاقًا من هذه المعطيات، يعالج هذا المطلب محورين مترابطين: **أولهما** :تحليل صعوبة إثبات العلاقة السببية بين الخطأ والضرر في بيئة الانتهاكات الرقمية للبيانات الشخصية، مع إبراز المعالجات القضائية المقارنة؛ **وثانيهما** :بيان صور المسؤولية المدنية – عقدية كانت أو تقصيرية – التي يمكن أن تُرتّب التزامًا بالتعويض، مع تحليل الآليات المتاحة لحماية المتضررين وسبل تطويرها.

8. أولًا: إثبات العلاقة السببية بين الخطأ والضرر

.1التأســـيس **المدني للعلاقة الســـببية في المعالجة الرقمية : يُعد ركن العلاقة الســـببية أحد الأركان الحاسمة في بناء المسؤولية المدنية، إذ لا يكفي قيام الخطأ وحده، أو تحقق الضـــرر بمفرده، بل يجب أن يثبت أن هناك رابطة منطقية وقانونية بين الفعل والنتيجة. وقد اســـتقرت القوانين المدنية العربيـة التقليـديـة – كـالمـادة (163) من القـانون المـدني المصـــري، والمـادة (204) من القـانون المدني العراقي، والفصل (78) من قانون الالتزامات والعقود المغربي – على ضـــرورة هـذا الارتبـاط المباشـــر. إلا أن هذا الفهم الكلاســـيكي يواجه تحديات جســـيمة عند تطبيقه على بيئة المعالجة الرقميـة، خـاصـــــةً مع تعـدد الفـاعلين التقنيين، واعتماد** المعالجة على نظم ســـحابية متداخلة قد تؤدي إلى تسرب البيانات أو إساءة استخدامها دون تحديد واضح للمسؤولية.

في الواقع، قد يحدث الخطأ من جهة، ويقع الضرر لاحقًا أو نتيجة لسلسلة تداخلات فنية تجعل إثبات الســببية المباشــرة أمرًا مرهقًا، بل غير ممكن في كثير من الحالات. من هنا نشـــأت الحاجة إلى تبنّي ما يُعرف بـــ"السببية المفترضة" أو "الوظيفية"، وهي التي تأخذ بها التشـــريعات الحديثة، كما في المادة (82) من اللائحة العامة لحماية البيانات في الاتحاد الأوروبي(GDPR) ، والتي تقضـــي بأن عبء إثبات انعدام المسؤولية يقع على عاتق المعالج حـال ثبوت وقوع خرق (European Union, 2016, Art. 82).

وقد كرّست محكمة العدل الأوروبية هذا المفهوم في قضـية Google Spain SL v. AEPD and Mario Costeja González (C-**131/12)**، حيث رأت أن اســتمرار ظهور بيانات شـخصـية في نتائج البحث رغم طلب حذفها، يشـكّل ضـررًا معنويًا ذا علاقة سـببية وظيفية بسـلوك مزود الخدمـة، ولو لم يثبت ضـــرر مـادي مبـاشـــر (CJEU, 2014).

.2التحديات العملية لإثبات العلاقة السببية في البيئة الرقمية

تتعدد التحديات التي تواجه المتضرر في إثبات العلاقة السببية في سياق انتهاكات البيانات الرقمية، وأبرزها:

- **غموض الفاعل التقني :**استخدام المعالجة لخوارزميات أو وسطاء يجعل تعيين المسؤول المباشر أمرًا صعبًا.
- **تأخر ظهور الضرر :**غالبًا لا يظهر الضرر الرقمي فور حدوثه، مما يعقّد إثبات العلاقة الزمنية بين الفعل والنتيجة.
- **الانتشار الفيروسي للبيانات :**سرعة تداول البيانات تضعف الرابط السببي المباشر.
- **غياب الدليل التقليدي :**الأدلة في البيئة الرقمية تكون رقمية وغير ملموسة، مما يجعل القرائن التقنية ضرورية.

وقد اســتجابت بعض الأنظمة القضــائية لهذه التحديات باعتماد مفهوم "انقلاب عبء الإثبات" لصالح المتضرر، كما في القانون الفرنسي الحديث الذي اعترف بالمفهوم في أحكام تتعلق بتســـريب بيانات طبية حساسـة (Cass. civ. 1ère, 11 octobre 2016)، وفي النظـام الألمـاني، حيـث اعتبرت المحكمة الفيدرالية في 2023 BGH VI) (125/22 ZRأن استخدام وسيلة غير مشفرة لنقل البيانات يُعد خطأً مفترضًـــا يتحمّل من ارتكبه عبء نفي العلاقة السببية.

3.المعالجة القضائية العربية والإقليمية المقارنة

في المغرب، بدأت محاكم الرباط والدار البيضاء في الأخذ بفكرة القرائن الفنية، واعتبار غياب أنظمة الحماية سببًا كافيًا لترتيب المسؤولية ولو كان الهجوم من طرف خارجي (محكمة الرباط، حكم 2021، مبطول، 2024، ص. 98). وفي مصر، وإن لم يقرّ المشرع بنظام خاص لإثبات السببية الرقمية، فإن محكمة النقض أقرت، في طعن رقم 4123 لسنة 89 ق (2020)، أن الإخلال بتدابير الحماية المتعارف عليها في المجال الرقمي يكفي لتحميل الجهة المتسببة المسؤولية المدنية.

أما العراق، فلا يزال يفتقر لتشريع خاص بالبيانات الرقمية، مما يدفع القضاء للرجوع إلى المادة (204) مدني، التي تشترط رابطة سببية مباشرة، وهو ما لا يتناسب مع طبيعة المخاطر الرقمية المركبة (الجبوري، 2023، ص. 122).

في المقابل، أقرت **الإمارات العربية المتحدة** في المادة (39) من قانون حماية البيانات رقم 45 لسنة 2021، أن عبء إثبات اتخاذ التدابير الكافية يقع على عاتق المعالج، ما يُعد تكريسًا لانقلاب عبء الإثبات لصالح صاحب البيانات. كما نصت اللائحة التنفيذية **لقانون البيانات السعودي (2021)** على توثيق جميع مراحل المعالجة إلكترونيًا، مما ييسر تتبع السبب ويخفف من عبء الإثبات عن المتضرر.

يتضح من التحليل السابق، أن أغلب الأنظمة العربية ما زالت تتبنى نموذجًا تقليديًا للعلاقة السببية، مما يضعف من فعالية الحماية القانونية للبيانات الرقمية. أما الاتجاه الأوروبي والخليجي الحديث، فقد ذهب نحو إعادة تأطير العلاقة السببية بمفهوم وظيفي يراعي التعقيدات التقنية، ويُخفف عبء الإثبات عن الضحية. ومن ثمّ، فإن تطوير النظام العراقي وغيره من الأنظمة المشابهة يتطلب تعديل النصوص المدنية بإدخال قواعد خاصة بقرائن العلاقة السببية في البيئات الرقمية، على غرار المادة 82 من**GDPR** ، مع توفير وسائل إثبات رقمية موازية للتقنيات الحديثة.

ثانياً: صور المسؤولية المدنية وآليات حماية المتضررين

لم تعد العلاقة القانونية بين صاحب البيانات والجهة المعالجة تقتصر على الرابطة التقليدية القائمة بين المدين والدائن في نطاق الالتزامات العامة، بل أصبحت تتخذ صورًا متباينة تُنتج آثارًا قانونية مختلفة من حيث التكييف والجزاء. ففي البيئة الرقمية، يمكن أن تنشأ المسؤولية المدنية عن الإخلال بضوابط معالجة البيانات في إطار **تعاقدي** يُرتّب التزامات محددة بناءً على اتفاق صريح أو ضمني بين الطرفين، كما هو الحال في الاشتراك بمنصة أو الموافقة على سياسة خصوصية. وفي المقابل، قد تقوم المسؤولية على أساس **تقصيري** حال غياب العلاقة التعاقدية أو في حال وقوع ضرر بفعل غير مشروع من جهة لا تربطها علاقة مباشرة بصاحب البيانات.

ويبرز هذا التعدد في صور المسؤولية المدنية كمظهر رئيسي لتطوّر مفاهيم الحماية في عصر البيانات، حيث إن طبيعة الفعل، وطبيعة الضرر، وتوزيع عبء الإثبات، ومدى الالتزام الواجب توافره، تختلف بحسب ما إذا كان الخطأ وقع في سياق التزامات تعاقدية محددة، أو بموجب إخلال عام بواجب قانوني أو تنظيمي (Bygrave, 2014, pp. 91–94; Fuster, 2014, p. 102).

وقد انعكس هذا التمييز في الممارسات التشريعية المقارنة؛ إذ نصت المادة (82) من **اللائحة العامة لحماية البيانات الأوروبية (GDPR)** على الحق في المطالبة بالتعويض، دون تقييد بالأساس القانوني، مما يفتح الباب للمساءلة المدنية سواء كانت تعاقدية أو تقصيرية (European Union, 2016). وفي النظام الفرنسي، ميّزت **محكمة النقض** في أحد أحكامها عام 2019 بين الإخلال بشروط الخدمة الذي يُعد خرقًا تعاقديًا، وبين الإخلال بتأمين المنصة ضد الهجمات الإلكترونية، والذي يُعد خطأً تقصيريًا مستقلًا (Cass. civ. 1ère, 2019). كما أكّد القضاء الأمريكي هذا التوجه في قضية In re Equifax، حيث أُقرّت ازدواجية المسؤولية نتيجة إخفاق الشركة في تأمين البيانات رغم تعهداتها التعاقدية.

أما في السياق العربي، فإن **القانون المصري رقم 151 لسنة 2020** لم يضع حدًا فاصلاً بين الصورتين، بل اعتمد معيار الإخلال بالضوابط كمدخل للمسؤولية المدنية، تاركًا التكييف للقضاء (محمود، 2024، ص. 1503). كما يسمح **القانون المغربي رقم 09.08** بمساءلة المعالج عن طريق أي من المسارين، بحسب طبيعة العلاقة القائمة (المبطول، 2024، ص. 113). وفي المقابل، لا يزال النظام العراقي يعتمد على مفاهيم تقليدية للمسؤولية المدنية دون تكييف واضح للمسؤولية الرقمية، مما يُبرز الحاجة إلى تطوير تشريعي يتماشى مع متطلبات العصر (الجبوري، 2023، ص. 137).

وتجدر الإشارة إلى أن بعض التشريعات الخليجية الحديثة، ولا سيّما في المملكة العربية السعودية ودولة الإمارات العربية المتحدة، قد بدأت تتخذ خطوات أكثر وضوحًا في تفعيل البعدين الوقائي والتعاقدي لحماية البيانات الشخصية، من خلال إصدار قوانين مستقلة تُلزم المعالجين باتخاذ تدابير فنية وتنظيمية مسبقة، وتقرّ مسؤوليتهم سواء بوجود عقد أو بدونه. فقد نصّ **القانون الاتحادي رقم 45 لسنة 2021 بشأن حماية البيانات الشخصية في الإمارات** على مجموعة من الالتزامات الصريحة بالشفافية، والحق في محو البيانات، وفرض قيود على النقل العابر للحدود (المادة 5 وما بعدها). كما أقرّ نظام حماية البيانات الشخصية السعودي الصادر بمرسوم ملكي رقم م/19 لعام 1443هـ بمسؤولية المعالج عن أي ضرر ناتج عن انتهاك أحكام النظام، بما في ذلك الضرر المعنوي، مع اعتماد مفهوم "الالتزام بالنتيجة" في بعض مواضعه، وتقنين الانقلاب الجزئي لعبء الإثبات في حالة الإخلال بضوابط الأمان أو الموافقة (المادة 39).

وهذا التوجه يعكس إدراكًا متقدّمًا لأهمية الحماية القانونية في بيئة المعالجة الرقمية، ويُبرز تمايزًا تشريعيًا مقارنةً ببعض الأنظمة العربية الأخرى – مثل العراق – التي ما زالت تفتقر إلى قوانين خاصة، أو تكتفي بالإحالة إلى القواعد المدنية العامة التي لا تواكب خصوصيات الواقع المعلوماتي الجديد.

وتظهر أهمية هذا التمييز في البيئة الرقمية المتسارعة، إذ تختلف **آليات الحماية** بحسب الصورة القانونية للمسؤولية: فبينما تشمل المسؤولية العقدية حق المطالبة بتنفيذ الالتزام أو التعويض عن الإخلال، تتيح المسؤولية التقصيرية مساحة أوسع لتعويض الضرر الأدبي أو النفسي، أو المطالبة بحذف البيانات أو وقف المعالجة.

وتأسيسًا على ما سبق، فإن التناول التالي سيتناول أولًا المسؤولية العقدية وما تفرضه من التزامات محددة على المعالج حال إخلاله بشروط الاستخدام أو الضوابط الفنية المتفق عليها، ثم ننتقل إلى دراسة المسؤولية التقصيرية وما تثيره من إشكاليات إثبات ومداها في حماية الحقوق الرقمية في غياب التعاقد.

1. المسؤولية العقدية: إخلال المعالج بالتزاماته الاتفاقية في سياق البيانات الشخصية

يتّضح من المقارنة بين النظم القانونية العربية والغربية في مجال حماية البيانات الشخصية أن الأنظمة الغربية، وعلى رأسها الاتحاد الأوروبي، قد بلغت مرحلة متقدمة من ترسيخ المسؤولية العقدية كآلية حمائية فعّالة، تتجاوز المفهوم التقليدي للضرر المادي إلى نطاق أوسع يشمل الأضرار المعنوية والتهديدات المستقبلية للخصوصية (Bygrave, 2014; Gellert, 2018). فقد كرّست المادة 82 من اللائحة العامة لحماية البيانات (GDPR, 2016) مبدأ "الالتزام بالنتيجة" في المعالجات التعاقدية، وأقرت بأن مجرد الإخلال بالالتزام يُرتب مسؤولية تعويضية حتى في غياب ضرر ملموس. ويُجسد ذلك بوضوح في قضية Ryanair DAC v. Booking.com BV (CJEU, 2022)، وأيضًا في القرار التاريخي ضد شركة Meta Platforms Ireland Limited لعام 2023، حيث فرضت المفوضية الأوروبية غرامة غير مسبوقة بلغت 1.2 مليار يورو بسبب خرق قواعد النقل العابر للبيانات.(Wired, 2023)

في المقابل، لا تزال النظم العربية تُراوح في منطقة التفسير الحَذِر للمسؤولية الرقمية، رغم صدور تشريعات حديثة نسبيًا في دول مثل السعودية (نظام حماية البيانات الشخصية، 2023) والإمارات (القانون الاتحادي رقم 45 لسنة 2021)، والتي ألزمت المعالجين بالتزامات صريحة تعاقديًا تتعلق بالحذف والأمان والشفافية (Akin Gump, 2023; DPO, 2024).

ومع ذلك، فإن القضاء في هذه الدول لم يبلغ بعد الدرجة المطلوبة من الاجتهاد في تأويل العقود الإلكترونية في ضوء المصلحة المعنوية للبيانات، ما يجعل تطبيق تلك النصوص في الواقع العملي محدودًا مقارنة بالاتجاه القضائي الغربي (Voigt & von dem Bussche, 2017, pp. 103–105).

ولعل هذا التفاوت الجوهري لا يعكس ضعفًا تشريعيًا بقدر ما يعكس فجوة فقهية وتأويلية، تفرض ضرورة إعادة هندسة الفهم العربي للعقد الإلكتروني، ليشمل خصوصية البيانات كمحلّ التزام تعاقدي صريح ومستقل، على نحو يُكرّس الحقوق الرقمية كأحد تجليات العدالة التعاقدية الحديثة (Voigt & von dem Bussche, 2017, p. 109). إن تفعيل القضاء العربي لهذا الدور لا يُحقق فقط امتثالاً دوليًا، بل يُعد خطوة استراتيجية لبناء الثقة الرقمية، وجذب الاستثمارات التكنولوجية في بيئة قانونية تضمن الحماية المسبقة واللاحقة للبيانات الشخصية.

ومن وجهة نظرنا، فإن تحليل التجربة المقارنة في مجال المسؤولية العقدية عن الإخلال بحماية البيانات الشخصية يكشف عن هوةٍ مفاهيمية وتشريعية واضحة بين ما بلغه الغرب من رُقيّ تشريعي وقضائي، وبين التناول التقليدي السائد في معظم الأنظمة العربية. ففي حين انطلقت اللائحة

الأوروبية (GDPR, 2016) من فلسفة تُؤسس لحق تعاقدي مستقل للخصوصية، يقوم على التزام إيجابي بالنتيجة، لا تزال الأنظمة العربية تُحجم عن منح هذا الحق ثقله الموضوعي داخل العلاقة التعاقدية، سواء بفعل غياب النصوص أو ضعف التفعيل القضائي لها.(Bygrave, 2014; Gellert, 2018)

ويُعد النظام القانوني العراقي مثالًا بالغ الدلالة على هذا التفاوت؛ إذ لم يُصدر بعد تشريعًا خاصًا بحماية البيانات الشخصية، بل يستند في معالجة هذا النوع من النزاعات إلى القواعد العامة في القانون المدني (المواد 125–130)، التي لا تُراعي خصوصيات العقود الإلكترونية ولا طبيعة المعالجات الرقمية للبيانات .(Al-Shammari, 2023, pp. 88–89)

وهو ما يجعل الالتزامات المفترضة على المعالج – كالحذف، وعدم الإفشاء، والحد من الغرض – التزامات غير قابلة للتقاضي الصريح، إلا من خلال تكييفات اجتهادية غير مستقرة، مما يُضعف من فاعلية الحماية ويُفرغ مبدأ الخصوصية من أثره التعاقدي.

ويكمن الخطر الأكبر في استمرار هذا الوضع دون تدخل تشريعي عاجل، خاصة في ضوء ازدياد الاعتماد المؤسسي على نظم الذكاء الاصطناعي، وتحول البيانات إلى أصل تجاري بالغ القيمة. إن غياب منظومة قانونية تُقنّن هذه المسؤولية تعاقديًا، وتُفعّل أدوات الإنفاذ القضائي بشأنها، يُعد تقاعسًا عن حماية مصلحة اجتماعية محورية، ويحول دون اندماج الدول العربية – ومنها العراق – في الاقتصاد الرقمي العالمي القائم على الثقة والامتثال.(DPO, 2024; Gellert, 2018)

وختامًا، فإن تكريس المسؤولية العقدية عن حماية البيانات في الأنظمة العربية لا يُعد ترفًا قانونيًا، بل هو ضرورة حمائية واقتصادية وسيادية، تقتضي تحركًا تشريعيًا فوريًا يُعيد تعريف العلاقة التعاقدية في البيئة الرقمية، ويجعل من حماية الخصوصية التزامًا جوهريًا يُرتب المسؤولية بمجرد الإخلال، ولو دون تحقق ضرر مادي مباشر، على غرار ما أرسته المحاكم الأوروبية مؤخرًا في قضايا Clearview AI (The Verge, 2024; وMeta Wired, 2023).

2–المسؤولية التقصيرية: تأصيل مفهومي وتجديد تشريعي لحماية الحق في الخصوصية الرقمية

بينما تُعدّ المسؤولية العقدية في معالجة البيانات الرقمية وسيلة حمائية مرتبطة بوجود علاقة قانونية سابقة، فإن المسؤولية التقصيرية تمثل الأساس القانوني الأصيل لحماية الحقوق الرقمية في الحالات التي تغيب فيها الروابط الاتفاقية أو تكون غير كافية. ويستند هذا النوع من المسؤولية إلى الفعل الضار المستقل الذي يعتدي على مركز قانوني محمي، وتحديدًا "الحق في الخصوصية" و"التحكم بالمعلومة الشخصية" كمصاديق حديثة للحقوق المدنية غير المالية (Bygrave, 2014; Voigt & von dem Bussche, 2017).

وقد شهدت الأنظمة الغربية تحولًا جذريًا في فهم المسؤولية التقصيرية في سياق البيانات، بحيث لم تعد قاصرة على تعويض الأضرار المادية أو المعنوية

الظاهرة، بل اتجهت إلى تبني معيار وقائي يرتب المسؤولية على مجرد الإخلال بالتزامات الحيطة المعلوماتية. ففي قضية Lloyd v. **Google LLC** أمام المحكمة العليا البريطانية (UKSC, 2021)، أُقرت مسؤولية الشركة عن جمع بيانات المستخدمين دون موافقتهم، رغم عدم إثبات ضرر فردي مباشر، استنادًا إلى "الضرر الجماعي غير المادي"، وهو مفهوم أحدث نقلة نوعية في تصور الضرر المعلوماتي.

أما في الولايات المتحدة، فتمثّل قضية Facebook Consumer Privacy User Profile Litigation (N.D. Cal., 2022) محطة محورية في تعزيز الأساس التقصيري، إذ أقرت المحكمة حق المستخدمين في التعويض عن "إساءة استخدام بياناتهم من طرف ثالث" حتى لو لم يكونوا على علم مباشر بالفعل، ما دام هناك إخلال بواجب الإفصاح الأمني من جانب مزود الخدمة (FTC, 2022).

في المقابل، لا تزال الأنظمة العربية – بما في ذلك المصرية والعراقية – تُحجم عن الاعتراف المستقل بالخصوصية الرقمية كحق غير مالي خاضع للمساءلة التقصيرية، وتُحيل أغلب الانتهاكات إلى قواعد الضرر التقليدي المنصوص عليها في المواد العامة (م 163 مدني مصري، م 204 مدني عراقي). وهو ما يجعل إثبات الضرر الرقمي، في ظل غياب التعاقد أو وضوح الخطأ، أمرًا عسيرًا من الناحية الإجرائية، ويُضعف فاعلية الحق في الحماية.

إلا أن بعض البوادر القضائية تشير إلى تحول تدريجي. ففي حكم لمحكمة دبي المدنية(2022) ، قضت المحكمة بمسؤولية إحدى الشركات التقنية عن تسرب بيانات حسابات مستخدمين بسبب إخفاقها في تحديث بروتوكولات التشفير، رغم عدم وجود عقد مباشر مع المستخدمين، مستندة إلى أن "الإخلال بواجب العناية السيبرانية" يُعد خطأ تقصيريًا مستقلاً.(DIFC Judgments, 2022) كما صدرت عن **محكمة عمان الابتدائية (2021)** أحكام جزئية تُقر بضرورة تعويض مستخدمين عن أضرار معنوية ناتجة عن مشاركة بياناتهم الصحية دون موافقة، وإن كانت لا تزال هذه الاجتهادات محدودة في مدى امتدادها النظري والتطبيقي.(Al-Khatib, 2023)

ومن منظور نقدي، فإن الإشكال الأعمق لا يكمن فقط في نقص التشريع، بل في **جمود التأويل القضائي للنصوص المدنية العامة**، وعدم مرونة قواعد الإثبات التقليدية أمام خصوصية الضرر الرقمي. لذا، بات من الضروري – كما أخذت به محكمة العدل الأوروبية – اعتماد **مبدأ الخطأ المفترض** أو **الضرر الاحتمالي** في قضايا البيانات، لا سيما في الحالات التي يكون فيها الإخلال جليًا من الناحية التقنية، وإن غابت العلاقة المباشرة بين المعالج والمتضرر (European Data Protection Board, 2022).

ختامًا، فإن إعادة بناء المسؤولية التقصيرية في البيئة الرقمية لا يجب أن تقتصر على إدراج نصوص تشريعية جديدة، بل تتطلب **تحولًا نوعيًا في الفقه والقضاء العربي** نحو الاعتراف بالهوية الرقمية كمحل حماية مدنية قائمة بذاتها، يترتب على المساس بها قيام مسؤولية مستقلة تُنصف الضحايا وتُرهب المعتدين، دون اشتراط وجود عقد، أو إثبات ضرر مالي مباشر.

ملاحظات ختامية:

في ضوء ما تقدم، يتّضح أن العلاقة السببية وصور المسؤولية المدنية في المعالجة الرقمية للبيانات تُشكّلان حلقة مركزية في بناء نظام حمائي فعّال يوازن بين متطلبات التقنية ومبادئ العدالة القانونية. فقد كشفت المقارنة بين النظم الغربية والعربية عن تباين جوهري في النظرة إلى الضرر الرقمي وطبيعة العلاقة بين المعالج والمتضرر؛ ففي حين ذهبت أنظمة الاتحاد الأوروبي والأنجلوساكسونية إلى تكريس مفاهيم متقدمة كالسببية المفترضة والضرر غير المادي الجماعي، لا تزال الأنظمة العربية – باستثناء بعض الاجتهادات القضائية في المغرب والإمارات – أسيرة المفاهيم التقليدية التي تُقصر السببية على العلاقة المباشرة، والمسؤولية على القواعد العامة.

Facebook و Privacy Google Litigation، أن التقاضي في البيئة الرقمية يحتاج إلى إطار نوعي جديد، يُعيد تعريف العلاقة بين الأطراف، ويُقرّ بمبدأ المسؤولية "الوقائية" لا "الزجرية" فقط، ويُوسع نطاق الحماية ليشمل الحقوق المعنوية والهوية المعلوماتية.

وعليه، فإن تطوير النظام القانوني العراقي، ومعه بقية الأنظمة المدنية العربية، يقتضي ليس فقط **استحداث نصوص خاصة**، بل تبنّي فلسفة قانونية جديدة تنطلق من الآتي:

- الاعتراف بالخصوصية الرقمية كحق مدني مستقل غير تابع.
- إدراج معيار الضرر المعلوماتي ضمن صور الضرر القابلة للتعويض.

تفعيل الخطأ المفترض في بيئة المعالجة، وتخفيف عبء الإثبات عن المتضرر.

- استحداث هيئات قضائية أو متخصصة للفصل في منازعات المعالجة.
- تعزيز مسؤولية المعالج حتى في غياب العقد، عبر تقنين الالتزامات الأمنية والتنظيمية.

إن هذه الخلاصة لا تُغلق النقاش، بل تفتحه على ضرورات تشريعية وفقهية عاجلة، تضمن أن لا يكون الحق في البيانات مجرد امتياز رقمي، بل حقًا مدنيًا مركزيًا، تُبنى عليه الحماية، وتُفهم في ضوئه المسؤولية، ويُعاد من خلاله ضبط التوازن بين الفرد والمنصات الرقمية.

الخاتمة

لقد أظهر التحليل المقارن للمسؤولية المدنية الناشئة عن معالجة البيانات الشخصية الرقمية أن النظم القانونية المعاصرة تشهد تحولًا نوعيًا في إدراك طبيعة البيانات الرقمية، لا بوصفها مجرد معلومات تقنية، بل كامتدادات قانونية ووجودية لهوية الفرد. هذا التحول استوجب مراجعة جذرية للأطر التقليدية للمسؤولية المدنية، لا سيما في ظل بيئة رقمية تتسم بالتشظي التقني، وتداخل الأدوار بين المتحكمين والمعالِجين، وتجاوز المعالجة للحدود السيادية للدول.

وقد سعى البحث إلى معالجة إشكالية مركزية مفادها :ما مدى كفاية الأطر القانونية الحالية – ولا سيما في النظام العراقي – في تنظيم المسؤولية المدنية عن المعالجات غير المشروعة للبيانات الشخصية الرقمية؟، وذلك عبر تحقيق أهداف متكاملة تشمل: تحليل الطبيعة القانونية للبيانات الرقمية، تفكيك أركان المسؤولية، وبيان صورها الحديثة، وانتهاءً بتقديم مقترح إصلاحي تشريعي متكامل.

أولًا: النتائج

- تكييف البيانات الشخصية كحق مدني غير مالي: أكدت الدراسة أن الاتجاه المقارن، وفي مقدمته اللائحة العامة لحماية البيانات(GDPR) ، يُقر بالبيانات الشخصية كحق أصيل، لصيق بالشخصية القانونية، ما يوجب بناء مسؤولية خاصة، تنشأ من مجرد الإخلال بضوابط المعالجة دون الحاجة لإثبات ضرر تقليدي.
- **قصور** المنظومة العربية – ولا سيما العراقية – عن مواكبة المفاهيم الحديثة: كشف التحليل عن تأخر تشريعي ملحوظ في عدد من الأنظمة العربية، من بينها العراق، في تقنين حماية البيانات الشخصية أو الاعتراف بالخصوصية الرقمية كحق مدني مستقل. وقد أدى هذا الفراغ إلى صعوبة، بل استحالة، مساءلة الجهة المعالجة عن الإخلال، في ظل غياب المعايير القانونية الفنية أو آليات الإثبات المتخصصة. وفي مقابل هذا القصور، يُلاحظ أن المملكة العربية السعودية ودولة الإمارات العربية المتحدة تتخذان خطوات أكثر وضوحًا نحو تفعيل الحماية الوقائية والتعاقدية للبيانات، من خلال تشريعات حديثة، وهيئات تنظيمية، ولوائح تنفيذية تُعزز الامتثال وتُيسر المساءلة، ما يضعهما في طليعة الدول العربية في هذا المجال.
- **اتساع** نطاق الخطأ المدني في البيئة الرقمية: أظهرت التطبيقات المقارنة أن الخطأ في المعالجة لم يعد مقتصرًا على صور الإهمال أو الإفشاء، بل يشمل أيضًا مخالفة مبادئ الشفافية، أو المعالجة بدون غرض مشروع، أو الإخلال بالتناسب، ولو دون تحقق ضرر مادي.
- **صعوبة** إثبات العلاقة السببية تستوجب قلب عبء الإثبات: أكدت النماذج القضائية الغربية على ضرورة اعتماد مفهوم "السببية المفترضة" في النزاعات الرقمية، ما يُخفف العبء عن الضحية، ويُلزم الجهة المعالجة بإثبات التزامها بالإجراءات الوقائية، بدلًا من مطالبة المتضرر بإثبات الضرر المباشر.
- **تنوع** صور المسؤولية يقتضي بناء منظومة مزدوجة: أظهرت الدراسة أهمية التفرقة بين المسؤولية العقدية – متى وُجد اتفاق – والمسؤولية التقصيرية – حال غياب العلاقة التعاقدية – مع تطوير منظومة متكاملة تُراعي طبيعة العلاقة، وتنوع آثار الإخلال، وآليات الإثبات في كل حالة.
- **غياب الإطار** المؤسسي في العراق يشكل فراغًا وظيفيًا: لا يملك العراق حتى الآن جهازًا وطنيًا لحماية البيانات، ولا توجد لوائح تنظيمية أو منصة شكاوى أو آلية فنية لمتابعة الانتهاكات، ما يُضعف من جدوى أي مساءلة مدنية مهما بلغت جسامة الضرر.

ثانيًا: التوصيات

1. **تعديل القانون المدني العراقي** لإدراج نص صريح يُقر بالبيانات الشخصية كحق غير مالي مستقل، يرتب مسؤولية قانونية بمجرد الإخلال، دون اشتراط ضرر مادي.
2. **إصدار قانون خاص لحماية البيانات الرقمية**، يضم المبادئ الحديثة مثل الموافقة الصريحة، وتحديد الغرض، والحق في النسيان، والمراجعة، والشفافية.
3. **إنشاء هيئة وطنية مستقلة لحماية البيانات**، تتمتع بسلطات تنظيمية ورقابية، وتكون مرجعًا في تسوية المنازعات، وتطبيق الجزاءات.
4. **إدراج قواعد إثبات خاصة للمعالجة الرقمية**، تقوم على الخطأ المفترض، وتتيح للقضاء الاعتماد على الخبرات الفنية والقرائن التقنية.
5. **تعديل العقود المدنية لتضمين حماية البيانات كالتزام تعاقدي صريح**، خصوصًا في الاشتراكات الرقمية والتعاملات الإلكترونية.
6. **تطوير القضاء العراقي عبر وحدات رقمية متخصصة**، تتعامل مع النزاعات التقنية، وتعتمد على المعايير الدولية في حماية البيانات.
7. **تبني فلسفة وقائية للمسؤولية المدنية**، تُلزم المعالجين بتقييم دوري للمخاطر وتحديث بروتوكولات الحماية، والإخطار الفوري عند حدوث اختراق.

8. **إدماج موضوع المسؤولية الرقمية في المناهج الجامعية القانونية**، وتعزيز البحث الأكاديمي والتشريعي في هذا الحقل الحيوي.

ختامًا: لم تعد المسؤولية المدنية في البيئة الرقمية فرعًا تابعًا للنظرية العامة، بل غدت علمًا قانونيًا متماسكًا، يجمع بين الفقه المدني، والتشريع المعلوماتي، والضمانات الدستورية الحديثة. وإن كانت أوروبا وأمريكا قد قطعت أشواطًا في إعادة تعريف العلاقة بين الإنسان وبياناته، فإن العراق، ومعه أغلب الأنظمة العربية، بات مدعوًا لا إلى مجرّد اللحاق، بل إلى الانخراط في تأسيس فلسفة قانونية رقمية سيادية، تُعلي من كرامة الفرد المعلوماتية، وتُرسّخ الحق في الخصوصية كجزء لا يتجزأ من الحريات المدنية، وتُفعّل الحماية على مستوى النص والتقاضي والتنفيذ.

المصادر

أولاً : المراجع باللغة العربية:

أ- المقالات العلمية:

1. الجبوري، س. (2023). نحو تكييف قانوني مستقل للضرر المعلوماتي في القانون المدني العراقي .*مجلة العدالة العراقية*، *41*(3)، 114.-129

2. العيش، ص. م. (2023). حماية البيانات الشخصية في القانون الأوروبي .*مجلة كلية القانون الكويتية العالمية*، *11*(43)، 289.-322

3. علي، خ. م. (2023). الحماية القانونية للبيانات الشخصية في إطار القانون المدني: دراسة مقارنة .*مجلة كلية القانون للعلوم القانونية والسياسية*، *12*(47)، 227.-243

4. المبطول، م. (2024). المسؤولية المدنية عن انتهاك الخصوصية الرقمية: معالجة المعطيات الشخصية نموذجًا .*مجلة قراءات علمية في الأبحاث والدراسات القانونية والإدارية*، *27*، 71.-97

5. محمود، س. أ. (2024). حماية البيانات الشخصية الرقمية وفقًا لأحكام القانون المصري رقم 151 لسنة 2020 .*مجلة العلوم القانونية والاقتصادية*، 66(1)، 1439.-1482

ب- الكتب والدراسات المنشورة:

6. الجبوري، س. ع .(2011) .*الحماية القانونية لمعلومات شبكة الإنترنت* .بيروت: منشورات الحلبي الحقوقية.

7. الجبوري، سليم عبد الله .(2023) .*الحماية القانونية للبيانات الشخصية في إطار القانون المدني* .بيروت: منشورات الحلبي الحقوقية.

8. الخطيب، س .(2023) .*الخصوصية الرقمية والضمانات المدنية في التشريعات العربية* .عمّان: المعهد العربي للقانون.

9. سرور، أ. ف .(1975) .*الحق في احترام الحياة الخاصة* .القاهرة: دار النهضة العربية.

10. الشمري، أ .(2023) .*الحماية القانونية للبيانات الشخصية الرقمية في القانون المدني العراقي* .بغداد: دار الرافدين.

11. محمود، س .(2024) .*حماية البيانات الشخصية الرقمية وفقًا لأحكام القانون المصري رقم 151 لسنة 2020* .القاهرة: دار النهضة العربية.

12. مغربي، محمد .(2024) .*المسؤولية المدنية عن انتهاك الخصوصية الرقمية: معالجة المعطيات الشخصية نموذجًا* . الرباط: دار أبي رقراق.

ج- أعمال المؤتمرات:

13. براك، أ. م. (2024). الذكاء الاصطناعي والحق في الخصوصية الرقمية. في *أعمال مؤتمر التحديات والآفاق القانونية والاقتصادية للذكاء الاصطناعي*، كلية الحقوق – جامعة عين شمس

د- التشريعات والقوانين:

14. القانون المدني العراقي، المادة 204.

15. القانون المصري رقم 151 لسنة 2020 بشأن حماية البيانات الشخصية.

16. قانون حماية البيانات الشخصية المصري رقم2020/151،*الجريدة الرسمية–عددخاص*،2020

17. قانون 09.08 المتعلق بحماية المعطيات ذات الطابع الشخصي المغربي.
18. قانون حماية البيانات الشخصية الإماراتي، القانون الاتحادي رقم 45 لسنة 2021.
19. قانون حماية البيانات الشخصية السعودي، الصادر في 2023، مع لائحته التنفيذية.
20. نظام حماية البيانات الشخصية السعودي، المرسوم الملكي رقم م/19 بتاريخ 9 سبتمبر 2021.
21. الهيئة السعودية للبيانات والذكاء الاصطناعي. (2021). *نظام حماية البيانات الشخصية*.
22. الهيئة السعودية للبيانات والذكاء الاصطناعي (2021)*لائحة التنفيذية لقانون البيانات الشخصية*
23. مشروع القانون التونسي لحماية البيانات. (2023). وزارة تكنولوجيا الاتصال.

هـ- الأحكام القضائية:

24. محكمة النقض المصرية، الطعن رقم 4123 لسنة 89 ق، جلسة 2020.

ثانياً: المراجع الأجنبية:

أ-كتب وأعمال أكاديمية

1. Bougeard, A. (2021). *Le phénomène de Big Data et le Droit* (Doctoral thesis). Université de Strasbourg.
2. Bygrave, L. A. (2014). *Data Privacy Law: An International Perspective*. Oxford University Press.
3. Bygrave, L. A. (2014). *Data Protection Law: Approaching Its Rationale, Logic and Limits*. Kluwer Law International.
4. Cassinari, A. (2022). Il danno non patrimoniale nella protezione dei dati personali. *Rivista Italiana di Diritto Civile*.
5. Desgens-Pasanau, G. (2015). *La protection des données personnelles*. LexisNexis.
6. Fuster, G. G. (2014). *The Emergence of Personal Data Protection as a Fundamental Right of the EU*. Springer.
7. Gutwirth, S., & De Hert, P. (2010). *Data Protection in a Profiled World*.
8. Voigt, P., & von dem Bussche, A. (2017). *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer.

B. مقالات علمية ودراسات بحثية

9. Gellert, R. (2018). The Risk-Based Approach to Data Protection. *Oxford Internet Institute Research Paper*.
10. Gellert, R. (2018). Understanding the Notion of Risk in the GDPR. *Computer Law & Security Review, 34*(2), 274–283. https://doi.org/10.1016/j.clsr.2017.12.002

11. Hildebrandt, M. (2008). Profiling and the Rule of Law. *Identity in the Information Society, 1*(1), 55–70.

ب–تشريعات أوروبية ودولية

12. Council of Europe. (1950). *European Convention on Human Rights*.
13. European Union. (2000). *Charter of Fundamental Rights of the European Union*.
14. European Union. (2016). *General Data Protection Regulation (GDPR), Regulation (EU) 2016/679*.
15. European Union. (2016). *General Data Protection Regulation (GDPR), Article 82*.
16. European Union. (2016). *General Data Protection Regulation (GDPR), Articles 28, 82*.
17. European Parliament. (2021). *Artificial Intelligence and Civil Liability*. https://www.europarl.europa.eu
18. European Data Protection Board (EDPB). (2022). *Guidelines on Calculation of Fines under GDPR*. https://edpb.europa.eu

ج–أحكام قضائية أوروبية ودولية

19. Court of Justice of the European Union. (2014). *Google Spain SL v. AEPD and Mario Costeja González*, Case C-131/12.
20. Court of Justice of the European Union (CJEU). (2022). *Ryanair DAC v. Booking.com BV*, Case C-59/21.
21. Court of Justice of the European Union (CJEU). (2023). *Österreichische Post AG*, Case C-300/21.
22. Court of Justice of the European Union. (2023). Judgment on data controller's obligation of purpose limitation.
23. UK Supreme Court. (2021). *Lloyd v. Google LLC*, [2021] UKSC 50.
24. UK Supreme Court. (2021). *Lloyd v Google LLC*, UKSC 2019/0175.
25. Cass. civ. 1ère, 11 octobre 2016, France.
26. Cass. civ. 1ère, 13 février 2019, France.
27. BGH (2023), Az. VI ZR 125/22, Bundesgerichtshof, Germany.
28. Az. 12 O 267/22, LG Düsseldorf (2023).
29. RG n. 11775/2022, Tribunale di Milano (2022).
30. DIFC Judgments. (2022). XYZ Tech Data Breach Ruling. *Dubai International Financial Centre Courts*.
31. In re Equifax Inc. Customer Data Security Breach Litigation, 362 F. Supp. 3d 1295 (N.D. Ga. 2020).

د–هيئات رقابية وتقارير مؤسسات

32. Agencia Española de Protección de Datos. (2023). Resolution PS/00042/2023.
33. CNIL. (2019). Sanction against Google LLC for Lack of Transparency and Consent.
34. CNIL. (2022). Sanction against Clearview AI for unlawful use of biometric data.
35. Federal Trade Commission (FTC). (2019). Facebook to Pay $5 Billion Fine for Cambridge Analytica Data Violations.
36. Federal Trade Commission (FTC). (2022). Facebook User Privacy Litigation. https://www.ftc.gov

و–مقالات وتقارير صحفية ومواقع إلكترونية

37. Akin Gump. (2023). *UAE's New Federal Personal Data Protection Law: Key Highlights*. https://www.akingump.com
38. Akin Gump LLP. (2023). *Overview of Data Privacy Laws in the GCC*.
39. DPO Centre. (2024). *Overview of Gulf Data Protection Laws*. https://www.dpocentre.com
40. DPO Legal Commentary. (2024). *Data Law in the Gulf: Emerging Trends and Challenges*. *Gulf Law Journal*.
41. Reuters. (2022, December 23). *Facebook parent Meta to settle Cambridge Analytica scandal case for $725 million*. https://www.reuters.com
42. The Verge. (2024, March). *Clearview AI Faces New EU Legal Scrutiny over Facial Recognition Violations*. https://www.theverge.com
43. Varonis. (2024, November 15). *82 Must-Know Data Breach Statistics [updated 2024]*. https://www.varonis.com/blog/data-breach-statistics
44. Wired. (2023, May). *Meta Fined Record €1.2 Billion over Data Transfers*. https://www.wired.com

الملخص

يقر الاتجاه الحديث وفي مقدمته اللائحة العامة لحماية البيانات) (GDPR بالبيانات الشخصية كحق اصيل لصيق يالشخصية القانونية مايوجب بناء مسؤولية خاصة تنشأ من مجرد الاخلال بضوابط المعالجة دون الحاجة لاثبات ضرر تقليدي ، وقد كشفت الدراسة عن تأخر تشريعي ملحوظ في عدد من الانطمة ومنها النظام التشريعي في العراقيفي تقنين حمايةالبيانات الشخصية او الاعتراف بالخصوصية الرقمية كحق مدني مستقل وقد ادى هذا الفراغ الى صعوبة مسألة الجهة المعالجة عن الاخلال في ظل غياب المعايير القانونية الفنية او آليات الاثبات المتخصصة

الكلمات المفتاحية :- التطبيقات الرقمية , البيانات الشخصية الرقمية , معالجة البيانات الشخصية , المسؤولية القانونية , معالج البيانات الشخصية الرقمية.

Abstract

The modern trend, most notably the General Data Protection Regulation (GDPR), recognizes personal data as an inherent right inherent to legal personality, which necessitates the establishment of special liability arising from a mere breach of processing controls without the need to prove traditional harm. The study revealed a significant legislative delay in a number of systems, including the Iraqi legislative system, in codifying the protection of personal data or recognizing digital privacy as an independent civil right. This gap has made it difficult for the processing entity to sue for breaches in the absence of technical legal standards or specialized proof mechanisms

Keywords: Digital applications . Digital personal data , Personal data processing Legal liability of digital personal data processors.