



المسؤولية القانونية عن انتهاك البيانات الشخصية في البيئة الرقمية
دراسة مقارنة بين النظام السعودي والقانون المصري واللائحة الأوروبية (GDPR)

إعداد

فهد حاسن الأحمد
رقم الطالب: 253000565

Research Methods For Law

Supervised By

Nourallah Elkolaly

فهرس المحتويات

4.....	الملخص باللغة العربية:
4.....	Abstract (English):
5.....	المقدمة
5.....	أولاً: الخلفية
5.....	ثانياً: مشكلة البحث
6.....	ثالثاً: أهمية البحث
6.....	رابعاً: أهداف البحث
6.....	خامساً: منهجية البحث
7.....	الباب الأول: الإطار المفاهيمي للبيانات الشخصية والخصوصية الرقمية
7.....	الفصل الأول: ماهية البيانات الشخصية في التشريعات المقارنة
7.....	المبحث الأول: التعريف التشريعي للبيانات الشخصية
11.....	المبحث الثاني: أنواع البيانات الشخصية والتمييز بينها
12.....	الفصل الثاني: الطبيعة القانونية للبيانات الشخصية وخصائصها في البيئة الرقمية
13.....	المبحث الأول: الخصائص المميزة للبيانات الرقمية
14.....	المبحث الثاني: الطبيعة القانونية للحق في حماية البيانات
15.....	الباب الثاني: الحماية النظامية والقانونية للبيانات الشخصية (دراسة مقارنة)
15.....	الفصل الأول: التزامات جهة التحكم ومعالجة البيانات
15.....	المبحث الأول: مبادئ المعالجة المشروعة
16.....	المبحث الثاني: الالتزامات التقنية والإدارية (أمن البيانات)
17.....	الفصل الثاني: حقوق صاحب البيانات وآليات ممارستها
18.....	المبحث الأول: الحق في العلم والوصول

المبحث الثاني: الحقوق التصحيحية والنهائية (الحق في النسيان).....	18
الباب الثالث: المسؤولية القانونية عن انتهاك البيانات الشخصية.....	19
الفصل الأول: أركان المسؤولية التقصيرية عن الانتهاك الرقمي.....	19
المبحث الأول: الخطأ في معالجة البيانات.....	19
أولاً: العقوبات في النظام السعودي.....	20
ثانياً: العقوبات في القانون المصري.....	20
ثالثاً: العقوبات في اللائحة الأوروبية (GDPR).....	21
رابعاً: التطورات الحديثة في الإنفاذ.....	21
المبحث الثاني: الضرر وعلاقة السببية في الفضاء الافتراضي.....	22
الفصل الثاني: الجزاءات المقررة وآليات جبر الضرر.....	23
المبحث الأول: المسؤولية الجنائية والعقوبات النظامية.....	23
المبحث الثاني: المسؤولية المدنية والتعويض.....	24
الخاتمة والتوصيات.....	27
النتائج.....	27
التوصيات.....	28
قائمة المصادر والمراجع.....	29
أولاً: التشريعات والأنظمة.....	29
ثانياً: الدراسات والأبحاث الأكاديمية.....	29
ثالثاً: التقارير والمبادئ التوجيهية.....	30
رابعاً: المراجع الأجنبية.....	30

الملخص باللغة العربية:

تناول هذا البحث "المسؤولية القانونية عن انتهاك البيانات الشخصية في البيئة الرقمية" في ضوء الأنظمة الحديثة، وتحديدًا نظام حماية البيانات الشخصية السعودي والقانون المصري واللائحة الأوروبية (GDPR). استعرض البحث الماهية القانونية للبيانات وتصنيفاتها، ثم انتقل لتحليل الالتزامات الواقعة على جهات التحكم والحقوق المقررة للأفراد. وعالجت الدراسة أركان المسؤولية المدنية والجنائية المترتبة على الاختراقات والتسريبات الرقمية. وخلص البحث إلى أن مواجهة الانتهاكات تتطلب تضافر الجهود التقنية والقانونية، مع ضرورة تحديث القواعد التقليدية للمسؤولية لتستوعب الطبيعة المعنوية للبيانات.

Abstract (English):

This research examines the "Legal Liability for Personal Data Breach in the Digital Environment" in light of modern regulations, specifically the Saudi Personal Data Protection Law, the Egyptian Law, and the GDPR. The study explores the legal nature and classifications of personal data, analyzing the obligations of data controllers and the rights of data subjects. Furthermore, it addresses the elements of civil and criminal liability resulting from digital breaches and leaks. The research concludes that combating data violations requires a synergy between technical and legal efforts, emphasizing the need to update traditional liability rules to accommodate the intangible nature of digital data.

المقدمة

أولاً: الخلفية

تعد البيانات الشخصية في العصر الرقمي الركيزة الأساسية لكافة المعاملات الإلكترونية، حيث تجاوزت قيمتها الاقتصادية والاجتماعية الأصول المادية التقليدية. ففي ظل الثورة الرقمية والتحول نحو الاقتصاد القائم على البيانات، أصبحت المعلومات الشخصية سلعة ثمينة تُداول وتُجمع وتُعالج بكميات هائلة غير مسبوقة. ومع تسارع التحول الرقمي في المملكة العربية السعودية وجمهورية مصر العربية، ظهرت تحديات قانونية كبيرة تتعلق بحماية هذه البيانات من الانتهاكات الرقمية، خاصة مع التطور التقني الذي جعل الاختراقات أسهل وأسرع وعابرة للحدود.

تشكل البيانات الشخصية ركيزة أساسية في اقتصاد المعرفة، حيث تعتمد عليها الشركات التقنية ومنصات التواصل الاجتماعي ومؤسسات التجارة الإلكترونية في بناء نماذج أعمالها وتحقيق أرباحها. غير أن هذا الاعتماد المتزايد على البيانات يضع الأفراد في موقف ضعيف، إذ قد تُستخدم بياناتهم بطرق لا يعرفونها أو لا يوافقون عليها. وقد أظهرت الدراسات الحديثة أن معظم المستخدمين يمنحون موافقاتهم على سياسات الخصوصية دون قراءتها، مما يجعل الموافقة شكلية وغير حقيقية، وهو ما يستوجب تدخلاً تشريعياً لضمان حماية فعالة.

وتتجلى خطورة انتهاك البيانات الشخصية في أن الضرر الناتج عنها قد يكون دائماً وغير قابل للإصلاح، خاصة عندما تتعلق البيانات الحساسة مثل البيانات الصحية أو البنكية أو الحيوية. فسرقة الهوية الرقمية قد تؤدي إلى تدمير السمعة، وفقدان الثقة، وخسائر مالية فادحة، وأضرار نفسية عميقة. ولذلك، باتت حماية البيانات الشخصية تمثل أولوية قصوى للمشرعين في جميع أنحاء العالم، وعلى رأسهم المشرع الأوروبي الذي أصدر اللائحة العامة لحماية البيانات (GDPR) لتكون النموذج الأمثل الذي تحتذي به معظم التشريعات الوطنية.

ثانياً: مشكلة البحث

تركز المشكلة في التساؤل: إلى أي مدى استطاع المنظم السعودي والمشرع المصري مواءمة نصوصهما القانونية لحماية البيانات الشخصية بفاعلية ضد الانتهاكات الرقمية؟ وهل القواعد التقليدية للمسؤولية القانونية تكفي لتغطية الأضرار الناتجة عن مثل هذه الانتهاكات؟

وتتفرع عن هذا التساؤل إشكاليات فرعية عدة، منها: ما طبيعة المسؤولية القانونية عن انتهاك البيانات الشخصية في البيئة الرقمية؟ وهل العقوبات المقررة في النظامين السعودي والمصري كافية لتحقيق الردع العام والخاص؟ وإلى أي مدى تتوافق هذه الأنظمة مع المعايير الدولية وفي مقدمتها اللائحة الأوروبية (GDPR)؟ وما هي الآليات المناسبة لجبر الضرر الناشئ عن هذه الانتهاكات؟

ثالثاً: أهمية البحث

تكمن الأهمية في حادثة "نظام حماية البيانات الشخصية السعودي" الصادر بالمرسوم الملكي رقم (م/19) وتاريخ 1443/2/9هـ، والمعدل بالمرسوم الملكي رقم (م/148) وتاريخ 1444/9/5هـ، والحاجة إلى تأصيل أحكامه مقارنة بالقانون المصري واللائحة الأوروبية GDPR ، مما يساهم في تزويد الباحثين والقضاة بأطر عملية لمعالجة النزاعات التقنية المستحدثة.

كما تبرز أهمية هذه الدراسة في ظل التحول الرقمي المتسارع الذي تشهده المنطقة، وما يترتب عليه من تحديات قانونية غير مسبقة تتطلب فهماً عميقاً للأطر التشريعية المقارنة. ويُعد نظام حماية البيانات الشخصية السعودي أحد أبرز الخطوات التشريعية الحديثة التي تعكس توجه المملكة نحو تعزيز بيئة رقمية آمنة ومتوافقة مع أفضل الممارسات الدولية، ولا سيما في ظل رؤية السعودية 2030 التي تركز على بناء اقتصاد رقمي مزدهر ومستدام.

رابعاً: أهداف البحث

1. توضيح المفهوم القانوني للبيانات الشخصية وأنواعها وحمايتها في كل من النظام السعودي والقانون المصري واللائحة الأوروبية.
2. تحليل الالتزامات القانونية المترتبة على جهات التحكم والمعالجة.
3. دراسة حقوق صاحب البيانات وآليات ممارستها.
4. تفصيل المسؤولية القانونية المدنية والجنائية الناشئة عن الانتهاكات الرقمية.
5. تقديم توصيات لتطوير الأطر القانونية الوطنية بما يتوافق مع المعايير الدولية.

خامساً: منهجية البحث

يعتمد البحث على المنهج المقارن بين الأنظمة السعودية والمصرية واللائحة الأوروبية، إضافة إلى المنهج التحليلي للنصوص القانونية، والفقه القانوني، والدراسات الأكاديمية، وحالات الانتهاك الواقعية. وقد استخدم البحث المنهجين الوصفي والتحليلي المقارن بين مجموعة من القوانين الإجرائية، مع التركيز على الجوانب العملية لتطبيق هذه الأنظمة في الواقع.

الباب الأول: الإطار المفاهيمي للبيانات الشخصية والخصوصية الرقمية

يشكل هذا الباب المدخل النظري الأساسي لفهم موضوع البحث، إذ يتناول الإطار المفاهيمي للبيانات الشخصية في ظل التحول الرقمي المتسارع، وبيان ماهيتها، وطبيعتها القانونية، وخصائصها التي تميزها عن غيرها من البيانات التقليدية. وتكمن أهمية هذا الباب في كونه يؤسس للمفاهيم الأساسية التي تقوم عليها باقي أبواب البحث، خاصة فيما يتعلق بالمسؤولية القانونية وآليات جبر الضرر، إذ لا يمكن تحديد نطاق المسؤولية دون تحديد دقيق للموضوع المحمي وهو البيانات الشخصية وبيان خصائصه التي تجعله عرضة للانتهاك بطرق تختلف عن الانتهاكات التقليدية، وتتجلى قيمة هذا الباب أيضاً في كونه يضع الأسس النظرية التي تستند إليها الأحكام القانونية في البابين التاليين، حيث أن فهم طبيعة البيانات الشخصية وخصائصها في البيئة الرقمية هو الشرط الأساسي لفهم الالتزامات المقررة على جهات التحكم والحقوق المقررة لأصحاب البيانات، وكذلك لفهم أركان المسؤولية وآليات جبر الضرر.¹

الفصل الأول: ماهية البيانات الشخصية في التشريعات المقارنة

يتناول هذا الفصل الجانب التعريفي الأساسي للبيانات الشخصية، حيث يستعرض المفهوم التشريعي لها في كل من النظام السعودي والقانون المصري واللائحة الأوروبية (GDPR)، مع إجراء مقارنة تحليلية بين هذه النظم للوقوف على أوجه الاتفاق والاختلاف في تناولها لهذا المفهوم المحوري، ويبرز في هذا الفصل الاختلافات الدقيقة بين التشريعات الثلاثة، خاصة فيما يتعلق باتساع نطاق التعريف، ومدى شموله للبيانات الرقمية المستحدثة، وكيفية التعامل مع البيانات المشتقة التي تنتج عن دمج وتحليل البيانات، مما يعكس تنوع المناهج التشريعية في التعامل مع تحديات العصر الرقمي مع الحفاظ على جوهر الحماية المتمثل في صون كرامة الفرد وخصوصيته، ويتميز هذا الفصل بكونه يضع الإطار التعريفي الذي تنفرع منه جميع الأحكام القانونية في البحث، إذ أن أي التزام أو حق أو مسؤولية لا يمكن تحديدها بدقة دون تحديد دقيق لماهية البيانات الشخصية التي هي موضوع هذه الأحكام.

المبحث الأول: التعريف التشريعي للبيانات الشخصية

يُعد التعريف التشريعي للبيانات الشخصية بمثابة حجر الزاوية في أي نظام قانوني لحمايتها، فهو الذي يحدد نطاق تطبيق النظام، والأشخاص المشمولين بالحماية، ونوعية البيانات التي تخضع للأحكام الواردة فيه. فالدقة في التعريف ضرورية لتحديد الحقوق والالتزامات بوضوح، والمرونة ضرورية لمواكبة التطورات التقنية المتسارعة التي تظهر أنواعاً جديدة ومتطورة من البيانات لم يكن المشرع يتصورها عند وضع النص، ويتناول هذا المبحث التعريف التشريعي للبيانات الشخصية في ثلاثة أنظمة قانونية مختلفة، ويعقب ذلك مقارنة تحليلية بينها تكشف نقاط الالتقاء والاختلاف، وتبرز مزايا كل نظام في التعامل مع التحديات المرتبطة

¹ الصرايرة، تقوى فارس محمد، وحسن، حسام الدين محمود محمد. (2025). الطبيعة القانونية للمسؤولية عن انتهاكات البيانات الشخصية الإلكترونية والتعويض عنها. مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، العدد 92 ص 32 مسترجع من

https://jlr.journals.ekb.eg/article_509048

بهذا المفهوم المتجدد، مع التركيز على كيفية تحقيق التوازن بين الاتساع في التعريف لضمان حماية شاملة، والوضوح لتجنب الغموض الذي قد يؤدي إلى صعوبات في التطبيق العملي.

المطلب الأول: التعريف في نظام حماية البيانات الشخصية السعودي

في النظام السعودي الصادر بالمرسوم الملكي رقم (م/19) وتاريخ 1443/2/9هـ، المعدل بالمرسوم الملكي رقم (م/148) وتاريخ 1444/9/5هـ، تُحدد المادة الأولى البيانات الشخصية بأنها كل بيان يؤدي إلى التعرف على الفرد مباشرة أو غير مباشرة، بما يشمل الاسم، رقم الهوية، العناوين، أرقام التواصل، الحسابات البنكية، البطاقات الائتمانية، الصور الثابتة والمتحركة، وغيرها.² وقد جاء تعريف النظام السعودي شاملاً للبيانات الشخصية بأنها "كل بيان - مهما كان مصدره أو شكله - من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد أو يجعل التعرف إليه ممكناً بصفة مباشرة أو غير مباشرة". ويشمل التعريف بحسب المادة الأولى: الاسم، رقم الهوية الشخصية، العناوين، أرقام التواصل، أرقام الرخص والسجلات والممتلكات الشخصية، وأرقام الحسابات البنكية والبطاقات الائتمانية، وصور الفرد الثابتة أو المتحركة، بالإضافة إلى البيانات الصوتية والبيانات المتعلقة بالموقع الجغرافي عند استخدامها لتحديد هوية الفرد.

ويُعد هذا التعريف من أوسع التعريفات في التشريعات المقارنة، إذ لا يقتصر على البيانات التي تحدد الهوية بشكل مباشر، بل يمتد ليشمل كل ما يمكن أن يؤدي إلى التعرف على الفرد بشكل غير مباشر، بما في ذلك البيانات التي قد تبدو عادية ولكنها تصبح قادرة على تحديد الهوية عند دمجها مع بيانات أخرى. وهذا النهج يعكس فهماً عميقاً لواقع البيئة الرقمية، حيث أن البيانات المنفردة قد لا تبدو خطيرة، ولكن تجميعها وتحليلها قد يكشف عن هوية الفرد بالكامل، كما أن النظام السعودي يُعتبر البيانات الشخصية التي تم إخفاء هوية صاحبها بحيث لا يمكن التعرف عليه بأنها ليست بيانات شخصية، طالما أن عملية إخفاء الهوية تمت وفق الضوابط التي تحددها اللائحة التنفيذية. وهذا الاستثناء يهدف إلى تشجيع استخدام البيانات لأغراض البحث والتحليل الإحصائي، مع ضمان عدم إمكانية إعادة تحديد هوية الأفراد.³

ويستثني النظام أيضاً بعض الحالات من نطاق تطبيقه، مثل البيانات التي تعالجها الجهات الأمنية والقضائية لأغراض التحقيق والمحاكمة، والبيانات التي يعالجها الأفراد لأغراض شخصية أو منزلية، والبيانات المتعلقة بالكيانات الاعتبارية، وتهدف هذه الاستثناءات إلى تحقيق التوازن بين حماية الخصوصية والاعتبارات الأمنية والقضائية، وتكمن أهمية هذا التعريف الواسع في كونه يعكس رؤية المشرع السعودي في مواكبة التطورات التقنية المتسارعة، حيث لم يعد التعريف التقليدي للبيانات الشخصية قاصراً على الاسم ورقم الهوية فحسب، بل أصبح يشمل مجموعة واسعة من المعلومات التي باتت تُستخدم في تحديد هوية الأفراد في

² نظام حماية البيانات الشخصية السعودي، الصادر بالمرسوم الملكي رقم (م/19) وتاريخ 1443/2/9هـ، والمعدل بالمرسوم الملكي رقم (م/148) وتاريخ 1444/9/5هـ.

³ اللائحة التنفيذية لنظام حماية البيانات الشخصية، الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)

العصر الرقمي، كبيانات الموقع الجغرافي، وبصمات الأجهزة، وسجل التصفح، وأنماط الاستخدام، وغيرها من البيانات التي أصبحت تُجمع بشكل يومي من قبل المنصات الرقمية والتطبيقات الذكية.

المطلب الثاني: التعريف في القانون المصري

في القانون المصري رقم 151 لسنة 2020 بشأن حماية البيانات الشخصية، يشمل التعريف أي بيانات متعلقة بشخص طبيعي يمكن تحديده مباشرة أو عبر الربط مع بيانات أخرى. وقد عرفت التشريعات المصرية البيانات الشخصية بشكل متشابه مع التشريعات السعودية، مع التركيز على حماية خصوصية الأفراد وضمان حقوقهم في التحكم بمعلوماتهم الشخصية.⁴ ونص القانون المصري على أن البيانات الشخصية هي "كل بيان مهما كان مصدره أو شكله يتعلق بشخص طبيعي محدد أو قابل للتحديد". ويشمل ذلك على سبيل المثال لا الحصر: الاسم، رقم التعريف، عنوان السكن، رقم الهاتف، البريد الإلكتروني، الصور الشخصية، البيانات الصحية، والبيانات المتعلقة بالحالة العائلية، والبيانات المالية، والبيانات الحيوية، بالإضافة إلى معرفات الإنترنت مثل عنوان IP وملفات تعريف الارتباط، والبيانات المتعلقة بالموقع الجغرافي، والبيانات الصوتية.

ويُعد القانون المصري من التشريعات الحديثة نسبياً في مجال حماية البيانات الشخصية، وقد استفاد في صياغته من التجارب الدولية السابقة، خاصة اللائحة الأوروبية (GDPR) والنظام السعودي، مع مراعاة الخصوصية المصرية والظروف الاجتماعية والاقتصادية التي تميز المجتمع المصري. وقد جاء التعريف المصري متوافقاً مع المعايير الدولية، حيث ركز على عنصر "قابلية التحديد" كمعيار أساسي للبيانات الشخصية، وهو ما يتسق مع أغلب التشريعات المقارنة، ويتميز القانون المصري بمرونته في التعامل مع التطورات التقنية، حيث ترك الباب مفتوحاً لتفسير مفهوم "قابلية التحديد" ليشمل أي تطورات مستقبلية في وسائل التعرف على الأفراد. كما أن القانون المصري أعطى الأولوية لحماية البيانات الصحية والبنكية، مما يعكس اهتماماً خاصاً بالقطاعات الأكثر حساسية في المجتمع المصري.⁵

المطلب الثالث: المقارنة بين النظامين واللائحة الأوروبية

أولاً: أوجه الاتفاق بين النظام السعودي والقانون المصري:

كلا النظامين يستثنيان الأشخاص الاعتباريين ويقتصران على حماية الأشخاص الطبيعيين، وهما يتفقان أيضاً على أن البيانات الشخصية هي كل ما يمكن به تحديد هوية الفرد بشكل مباشر أو غير مباشر. كما يتفقان على ضرورة الحصول على موافقة صاحب البيانات قبل معالجتها، وعلى إقرار مجموعة من الحقوق لصاحب البيانات كالحق في الوصول والتصحيح والإتلاف، ويتفق النظامان أيضاً على إخضاع معالجة البيانات الحساسة لضوابط مشددة، وعلى ضرورة إبلاغ الهيئات الرقابية في حالة حدوث اختراقات للبيانات.

⁴ القانون المصري رقم 151 لسنة 2020، بشأن حماية البيانات الشخصية.

⁵ الرحيلي، رباب عبد الله. (2025). حماية البيانات الشخصية في البيئة الرقمية: دراسة مقارنة بين التشريعات العربية والدولية. المجلة الأمريكية الدولية للعلوم الإنسانية والاجتماعية. مسترجع من <https://iaiphss.us/>

ثانياً: أوجه الاختلاف بين النظامين:

1. مدة السماح للامتثال: منح النظام السعودي مهلة زمنية للجهات للامتثال لأحكامه، بينما كان القانون المصري أكثر إلحاحاً في التطبيق.
2. الرقابة: يُعهد بالرقابة في السعودية إلى الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) التي تتمتع بصلاحيات واسعة، بينما في مصر لا يزال إنشاء الهيئة الوطنية لحماية البيانات الشخصية قيد التفعيل.
3. شدة العقوبات: النظام السعودي يتضمن عقوبات سالبة للحرية (السجن) مع غرامات مالية عالية تصل إلى 3 ملايين ريال، بينما القانون المصري يجمع بين الحبس والغرامة ولكن بمبالغ أقل نسبياً.

ثالثاً: المقارنة مع اللائحة الأوروبية (GDPR)

تنص المادة (4) من اللائحة العامة لحماية البيانات (GDPR) على أن البيانات الشخصية هي "أي معلومة تتعلق بشخص طبيعي محدد أو يمكن تحديد هويته"، وتشمل على سبيل المثال: الاسم، رقم الهوية، بيانات الموقع، أو معرف الإنترنت كعنوان (IP)، أو عامل واحد أو أكثر من العوامل المادية أو الفسيولوجية، الجينية، النفسية، الاقتصادية، الثقافية أو الاجتماعية، وتتميز اللائحة الأوروبية عن النظامين السعودي والمصري بعدة نقاط:⁶

- النطاق الإقليمي الواسع الذي يمتد ليشمل أي جهة تعالج بيانات مواطني الاتحاد الأوروبي، بغض النظر عن موقعها الجغرافي.
- شمولية التعريف التي تشمل صراحةً بيانات الموقع الجغرافي ومعرفات الإنترنت.
- التفصيل الدقيق لمفاهيم مثل "البيانات الحيوية" و"البيانات الوراثية".
- فرض مبدأ "الخصوصية بالتصميم" كالتزام أساسي.
- نظام الغرامات النسبية التي تصل إلى 4% من حجم التداول السنوي.

ويلاحظ أن النظام السعودي يتميز بكونه أكثر توسعاً في تعداد الأمثلة على البيانات الشخصية، وهو ما يعكس حداته واستفادته من التجارب السابقة. أما القانون المصري فيتميز بمرونة تفسيرية تسمح بمواكبة التطورات المستقبلية دون الحاجة إلى تعديلات تشريعية متكررة.

⁶ الجيجلي، تمام عبداللطيف. (2025). حماية البيانات الشخصية للشركات والمؤسسات والأفراد وفقاً للمعايير الدولية وأحكام القانون الدولي الخاص. المجلة الدولية للعلوم والبحوث ص 32

المبحث الثاني: أنواع البيانات الشخصية والتمييز بينها

تتفاوت البيانات الشخصية في درجة حساسيتها، مما يستوجب تقسيمها إلى فئات لتحديد مستوى الحماية المناسب لكل فئة. فهذا التقسيم يسمح للمشرع بتخصيص التدابير الأمنية والقانونية وفقاً لطبيعة المخاطر المرتبطة بكل نوع من البيانات.

المطلب الأول: البيانات الشخصية العادية

البيانات الشخصية العادية هي تلك التي لا تنتم بالحساسية ولا تشكل خطراً جسيماً على خصوصية الفرد إذا تم الكشف عنها أو معالجتها بطريقة غير مشروعة. وتشمل: الاسم، العنوان، رقم الهاتف، البريد الإلكتروني، وتكون معالجتها مشروطة بموافقة صريحة أو سند قانوني. كما تشمل أيضاً بيانات الانتماء الوظيفي، والمؤهلات العلمية، والبيانات الديموغرافية الأساسية كالعمر والجنس، والبيانات المتعلقة بالمعاملات اليومية، وسجل الشراء، وتفضيلات المستهلك، وتاريخ التصفح العادي، ويشترط في معالجة هذه البيانات أن تكون محددة الأغراض، وأن يقتصر الجمع على القدر الضروري منها، وأن تلتزم جهة التحكم بمبدأ الشفافية والإفصاح عن كيفية استخدامها. ولا يُشترط لمعالجة هذه البيانات اتخاذ إجراءات مشددة كما هو الحال مع البيانات الحساسة، غير أن ذلك لا يعني إهمال حمايتها، إذ أن تسربها قد يؤدي إلى أضرار كبيرة خاصة إذا تم دمجها مع بيانات أخرى.⁷

وتجدر الإشارة إلى أن بعض التشريعات، مثل النظام السعودي، تُصنف البيانات المالية (كأرقام الحسابات البنكية والبطاقات الائتمانية) ضمن البيانات العادية، بينما تُصنفها تشريعات أخرى ضمن البيانات الحساسة، وهذا يعكس اختلافاً في النهج التشريعي حول مدى خطورة كل نوع من البيانات، كما أن مفهوم البيانات "العادية" هو مفهوم نسبي يتغير بتغير الظروف والسياقات؛ فقد يصبح رقم الهاتف بيانات حساسة إذا ارتبط بحسابات بنكية أو صحية، وقد يصبح العنوان بيانات حساسة إذا تم ربطه بانتماءات سياسية أو دينية، وقد أكدت دراسة الرحيلي (2025) أن التحدي الحقيقي لا يكمن فقط في حماية البيانات أثناء جمعها، بل في الحماية أثناء تحليلها ودمجها ضمن منظومات الذكاء الاصطناعي وقواعد البيانات الضخمة. فمثلاً، دمج سجل الشراء مع الموقع الجغرافي قد يكشف عن عادات صحية أو ميول سياسية للفرد، مما يجعله عرضة للاستهداف أو التمييز، وهذا يعني أن البيانات العادية قد تتحول إلى بيانات حساسة بمجرد دمجها مع بيانات أخرى، وهو ما يستوجب على المشرع أن يأخذه في الاعتبار عند وضع الضوابط التنظيمية.

المطلب الثاني: البيانات الشخصية الحساسة (البيانات المحظورة)

البيانات الحساسة هي تلك التي تكشف عن جوانب خاصة من حياة الفرد، والتي قد تؤدي معالجتها أو الكشف عنها إلى تمييز أو اضطهاد أو أضرار جسيمة. وتشمل: الأصل العرقي، المعتقدات الدينية، البيانات الجنائية،

⁷ إسماعيل، أماني مشهور. (2024) دور القانون الدولي لحقوق الإنسان في حماية خصوصية الأفراد: حق أساسي في العصر الرقمي [رسالة ماجستير غير منشورة]. جامعة الشرق الأوسط، الأردن ص 34

البيانات الحيوية والصحية، والبيانات المتعلقة بالحياة الجنسية للفرد. معالجة هذه البيانات مقيدة جداً، وانتهاكها يترتب عليه مسؤولية مدنية وجنائية صارمة.

وتشمل البيانات الحيوية: بصمة الإصبع، بصمة الوجه، الحمض النووي، وهي فريدة وتبقى ثابتة مدى الحياة، مما يجعل سرقتها كارثة لا يمكن إصلاحها، إذ لا يمكن تغيير بصمة الإصبع أو الحمض النووي كتغيير رقم الهاتف أو كلمة المرور. أما البيانات الصحية فتشمل السجلات الطبية والتشخيصات، والفحوصات المخبرية، والتاريخ الصحي للفرد، ولها قدسية خاصة في القانون السعودي والمصري، حيث يُعتبر الكشف عنها دون موافقة صاحبها انتهاكاً للكرامة الإنسانية. إن تسرب هذه البيانات قد يؤدي إلى أضرار دائمة للمواطن من الناحية المالية والنفسية، فقد يفقد فرصة عمل بسبب كشف مرضه، أو يتعرض للتمييز في التأمين الصحي، أو يُبتز عاطفياً أو مادياً.⁸

وتشمل البيانات الحساسة أيضاً البيانات المتعلقة بالحالة الاجتماعية والجنسية، والبيانات الوراثية، والانتماءات الحزبية والنقابية، والبيانات المتعلقة بالمعتقدات الفكرية، والبيانات المتعلقة بالأطفال، حيث تحظى باهتمام خاص في أغلب التشريعات، وتحظر الأنظمة الثلاثة معالجة هذه البيانات إلا في حالات استثنائية محددة، مثل الموافقة الخطية الصريحة من صاحبها، مع اشتراط أن تكون هذه الموافقة حرة ومستتيرة وقابلة للسحب في أي وقت، أو الضرورة لحماية حياة الفرد أو غيره، أو لأغراض صحية وقائية تحت إشراف طبيب مختص، أو لأغراض بحثية علمية مع ضمانات صارمة للسرية.

وتشترط الأنظمة الثلاثة لمعالجة البيانات الحساسة اتخاذ تدابير أمنية مشددة، تشمل التشفير المتقدم، وتحديد صلاحيات الوصول، وتقييد عدد الأشخاص المخولين بالاطلاع عليها، وتسجيل عمليات الدخول للتحقق من أي اختراق محتمل. كما تفرض الأنظمة الثلاثة عقوبات أشد على انتهاك البيانات الحساسة، سواء كانت عقوبات جنائية أو مدنية، وذلك لخطورة هذه البيانات وتأثيرها العميق على حياة الأفراد وكرامتهم.

الفصل الثاني: الطبيعة القانونية للبيانات الشخصية وخصائصها في البيئة الرقمية

يتناول هذا الفصل الخصائص المميزة للبيانات الرقمية والطبيعة القانونية للحق في حمايتها، مبيناً التحديات التي تفرضها هذه الخصائص على القواعد القانونية التقليدية. فالبيانات الرقمية تختلف جوهرياً عن الموضوعات القانونية التقليدية، مما يستوجب تطوير المفاهيم القانونية لمواكبة هذه الاختلافات.

⁸ القرشي، محمد الحسين. (2026). الإطار النظامي لحماية البيانات الشخصية في المملكة العربية السعودية وأثره على التزامات الجهات التقنية. المجلة الدولية للبحوث القانونية والاجتماعية ص 65

المبحث الأول: الخصائص المميزة للبيانات الرقمية

تتميز البيانات الرقمية بخصائص فريدة تجعل تطبيق القواعد القانونية التقليدية عليها أمراً صعباً، مما يستوجب تطوير هذه القواعد. هذه الخصائص هي التي تفسر لماذا لم تعد القواعد القانونية التقليدية كافية لحماية البيانات، ولماذا استوجب المشرعون استحداث قواعد خاصة تتناسب مع طبيعة هذه البيانات.

1. اللاتجسد: البيانات غير ملموسة، مما يصعب حيازتها بالمعنى التقليدي. ففي القانون المدني، تفترض قواعد الحيازة والاعتداء وجود شيء مادي يمكن السيطرة عليه، وهو ما لا يتوفر في البيانات الرقمية. فالبيانات لا يمكن "لمسها" أو "الاستيلاء عليها" بالمعنى المادي، مما يطرح إشكالية في تطبيق قواعد المسؤولية التقصيرية التي تقوم على أساس وجود شيء مادي يمكن الاعتداء عليه.

2. القابلية للنسخ اللامتناهي: النسخ لا يحرم صاحب البيانات، لكن الضرر يكمن في اطلاع الغير. فالبيانات الرقمية يمكن نسخها ملايين المرات بتكلفة صفرية تقريباً، مما يجعل السيطرة عليها شبه مستحيلة. وهذه الخاصية تجعل من الصعب تحديد مقدار الضرر، إذ أن الضرر لا يتمثل في فقدان الأصل بل في فقدان السيطرة على المعلومات.

3. العبور عبر الحدود: بيانات مواطن سعودي قد تعالج في خوادم خارجية، ما يثير إشكالية الاختصاص القضائي. ففي بيئة الإنترنت، لا تعترف البيانات بالحدود الجغرافية، مما يجعل تطبيق القوانين الوطنية أمراً صعباً، حيث قد تُخزن بيانات شخص في المملكة في خادم في أوروبا أو أمريكا، وتُعالج في الهند أو الصين.

4. القابلية للتحليل والتتبع: البيانات الرقمية يمكن دمجها وتحليلها لإنتاج معلومات شخصية إضافية. فما قد يبدو بيانات عادية بشكل منفرد، يمكن أن يكشف عن جوانب عميقة من حياة الفرد عند دمجها مع بيانات أخرى. فعلى سبيل المثال، دمج بيانات الموقع الجغرافي مع سجل المشتريات قد يكشف عن عادات غذائية أو حالات صحية أو حتى ميول سياسية.⁹

5. الديمومة: البيانات الرقمية لا تزول بمرور الزمن، بل تبقى مخزنة في الخوادم إلى ما لا نهاية، مما يجعل الأخطاء أو الانتهاكات مستمرة التأثير. فحتى بعد حذف البيانات، قد تبقى نسخ منها في خوادم أخرى أو في نسخ احتياطية، مما يجعل الحق في النسيان صعب التحقيق عملياً.

⁹ مدبولي، باسم محمد فاضل. (2024). المسؤولية التقصيرية عن معالجة البيانات الشخصية في البيئة الرقمية (دراسة مقارنة). المجلة الأردنية للقانون والعلوم السياسية ص 45

6. السرعة: تنتقل البيانات الرقمية بسرعة الضوء، مما يجعل الضرر يقع في لحظة قد لا يستطيع الفرد تداركها. فالاختراق يمكن أن يحدث في ثوانٍ، وينقل كميات هائلة من البيانات إلى أطراف غير مصرح لها، ويكون الضرر قد وقع قبل أن تتمكن جهة التحكم من اكتشافه أو إيقافه.

7. سهولة التعديل: يمكن تعديل البيانات الرقمية أو تزويرها بسهولة، مما يطرح تحديات في مجال الإثبات القضائي، حيث يصعب التمييز بين البيانات الأصلية والبيانات المعدلة.

8. الانتشار السريع: البيانات الرقمية تنتشر عبر الشبكات بسرعة فائقة، وقد تصل إلى ملايين الأشخاص في دقائق معدودة، مما يجعل الضرر الجماعي ممكناً.

هذه الخصائص الثماني تمثل تحديات كبيرة للقواعد القانونية التقليدية، حيث أن مفهوم "الحيازة" و"الاعتداء" في القانون المدني يفترضان وجود شيء مادي، بينما البيانات غير مادية. كما أن قابلية النسخ اللامتناهي تجعل من الصعب تحديد مصدر الضرر أو حصره، وقد بدأت بعض التشريعات الحديثة في التكيف مع هذه الخصائص من خلال استحداث مفاهيم جديدة كـ "الحق في تقرير المصير المعلوماتي" و"الحق في النسيان" و"الخصوصية بالتصميم".¹⁰

المبحث الثاني: الطبيعة القانونية للحق في حماية البيانات

تعددت الآراء الفقهية حول الطبيعة القانونية للحق في حماية البيانات بين اتجاه الملكية واتجاه الحقوق اللصيقة بالشخصية والاتجاه المزدوج. وهذا التعدد يعكس تعقيد الموضوع وتشعبه، إذ أن البيانات الشخصية تحمل في طياتها أبعاداً متعددة.

الاتجاه الأول: اتجاه الملكية: يرى أنصار هذا الاتجاه أن البيانات الشخصية هي حق ملكية معلوماتية، بمعنى أن الفرد يملك بياناته كما يملك أي أصل مادي، وله بالتالي الحق في التصرف فيها والاستفادة منها ومنع الآخرين من استخدامها دون إذنه. ويستند هذا الاتجاه إلى أن البيانات لها قيمة اقتصادية، وأن الأفراد يستثمرون بياناتهم في الحصول على خدمات مجانية، وأن حماية البيانات كملكية توفر حماية أقوى من حمايتها كحق شخصي.

الاتجاه الثاني: اتجاه الحقوق اللصيقة بالشخصية: يرى هذا الاتجاه أن الحق في حماية البيانات مشتق من الحق في الخصوصية، وهو من الحقوق اللصيقة بالشخصية التي لا يمكن التنازل عنها أو التصرف فيها. وهذا هو

¹⁰ رجب، هبة رمضان. (2024). الحماية القانونية للبيانات الشخصية في عصر التكنولوجيا الرقمية. مجلة العلوم القانونية والاقتصادية، كلية الحقوق جامعة عين شمس ص 46

الاتجاه الأكثر قبولاً في الفقه القانوني، ويطبقه النظام السعودي والمصري والأوروبي. فحماية البيانات جزء من حماية حقوق الإنسان وكرامته، وليس مجرد سلعة تجارية.

الاتجاه الثالث: الاتجاه المزدوج: يرى أصحاب هذا الاتجاه أن البيانات الشخصية تتمتع بطبيعة مزدوجة، فهي من جهة حق شخصي مرتبط بالكرامة والخصوصية، ومن جهة أخرى لها قيمة اقتصادية تجعلها قابلة للتداول والاستثمار. وهذا الاتجاه هو الأكثر ترجيحاً في الفقه الحديث، إذ يوفق بين البعدين ويحقق التوازن بين حماية الخصوصية وتشجيع الابتكار واستخدام البيانات في الاقتصاد الرقمي.¹¹

وتؤكد دراسة إسماعيل (2024) أن الحق في حماية البيانات الشخصية لم يعد شأناً محلياً، بل أصبح جزءاً من منظومة الحقوق الأساسية المعترف بها دولياً، وأن المعايير الدولية تفرض التزامات على الدول بسن تشريعات فعالة. وتتفق الأنظمة الثلاثة على أن الحق في حماية البيانات الشخصية هو حق أساسي من حقوق الإنسان، غير أن درجة هذه الحماية تختلف بين الأنظمة، حيث تُعد اللائحة الأوروبية الأكثر تقدماً من حيث التفاصيل والضمانات. وقد أكدت محكمة العدل الأوروبية في أكثر من مناسبة أن الحق في حماية البيانات الشخصية هو حق أساسي من حقوق الإنسان، وأن الدول ملزمة بحمايته من خلال سن تشريعات فعالة وإنشاء أجهزة رقابية مستقلة.

الباب الثاني: الحماية النظامية والقانونية للبيانات الشخصية (دراسة مقارنة)

يتناول هذا الباب الجانب العملي لحماية البيانات من خلال التزامات جهات التحكم وحقوق أصحاب البيانات وآليات ممارستها، وينقسم هذا الباب إلى فصلين رئيسيين: يتناول الفصل الأول التزامات جهة التحكم ومعالجة البيانات، بينما يتناول الفصل الثاني حقوق صاحب البيانات وآليات ممارستها.

الفصل الأول: التزامات جهة التحكم ومعالجة البيانات

يحدد هذا الفصل الالتزامات المقررة على جهات التحكم في مبادئ المعالجة المشروعة والتدابير التقنية والإدارية الواجب اتخاذها. وتقع على عاتق جهة التحكم مجموعة من الالتزامات الجوهرية التي تمثل جوهر حماية البيانات، فهي الضمانة الأساسية لحماية خصوصية الأفراد من الانتهاكات.

المبحث الأول: مبادئ المعالجة المشروعة

تشكل مبادئ المعالجة المشروعة الإطار الأخلاقي والقانوني الذي يجب أن تستند إليه أي معالجة للبيانات الشخصية، وهي ليست مجرد توصيات بل التزامات قانونية ملزمة. تفرض الأنظمة الثلاثة مجموعة من المبادئ التي تحكم معالجة البيانات الشخصية، وتتمثل في:

¹¹DLA Piper. (2026). GDPR Fines and Data Breach Survey 2025. DLA Piper.

1. مبدأ الغرض: جمع البيانات لأغراض محددة وواضحة، فلا يجوز استخدام البيانات لغرض آخر غير الذي جمعت من أجله دون موافقة صريحة من صاحبها. وهذا المبدأ يمنع استخدام البيانات بطرق غير متوقعة من قبل صاحبها.
2. مبدأ الحد الأدنى: الاكتفاء بالبيانات الضرورية فقط لتحقيق الغرض المحدد، وعدم جمع بيانات إضافية لمجرد الاحتمال أو التخزين المستقبلي. وهذا المبدأ يحد من كمية البيانات التي يتم جمعها، مما يقلل من مخاطر انتهاكها.
3. مبدأ الجودة والدقة: تحديث البيانات لمنع اتخاذ قرارات خاطئة، والتأكد من صحة البيانات قبل استخدامها في أي إجراء يؤثر على صاحبها. فالقرارات المبنية على بيانات غير دقيقة قد تؤدي إلى أضرار جسيمة للفرد.
4. مبدأ الشفافية: يلزم جهة التحكم بإعلام صاحب البيانات بكامل التفاصيل المتعلقة بمعالجة بياناته، بما في ذلك هوية الجهة، والغرض من المعالجة، ومدة الاحتفاظ، وحقه في سحب الموافقة. وهذا المبدأ يمكن الفرد من اتخاذ قرار مستنير بشأن بياناته.
5. مبدأ تقييد التخزين: يجب ألا تحتفظ جهة التحكم بالبيانات لفترة أطول مما هو ضروري لتحقيق الغرض. وقد نصت المادة التاسعة من اللائحة التنفيذية على حق صاحب البيانات في طلب إتلاف بياناته عند انتهاء الغرض.
6. مبدأ المسؤولية: يلتزم مراقب البيانات بأن يكون قادراً في أي وقت على إثبات امتثاله لكافة المبادئ السابقة، وهو ما يُعرف بمبدأ "الإثبات" أو "المساءلة".
7. مبدأ النزاهة والسرية: يجب معالجة البيانات بطريقة تضمن أمنها وسريتها، ومنع الوصول غير المصرح به أو الإفصاح غير المشروع.

التزامات الرقابة الداخلية: مراجعة دورية للبيانات، وضمان شفافية التعامل عند نقل البيانات لدول أخرى. وقد أصدرت الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) في 25 فبراير 2025 مجموعة شاملة من المبادئ التوجيهية التي تهدف إلى ضمان حماية البيانات الشخصية عند نقلها أو الإفصاح عنها لكيانات خارج المملكة. وتشمل هذه المبادئ أربع مراحل لتقييم المخاطر: مرحلة الإعداد، وتقييم الآثار السلبية والمخاطر المحتملة، وتقييم مخاطر نقل البيانات، والمبادئ التوجيهية لتحديد العوامل المتعلقة بتحليل الآثار على المصالح الحيوية للمملكة.¹²

المبحث الثاني: الالتزامات التقنية والإدارية (أمن البيانات)

تتطلب حماية البيانات اتخاذ تدابير تقنية وإدارية ملموسة تضمن أمنها وسلامتها من الاختراق والتسريب. وهذه التدابير تمثل الجانب العملي للحماية، وهي التي تحدد مدى فعالية النظام القانوني في مواجهة التحديات التقنية.

¹² الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا). (2025) المبادئ التوجيهية لتقييم مخاطر نقل البيانات الشخصية إلى خارج المملكة.

تفرض الأنظمة الثلاثة التزامات تقنية وإدارية على جهات التحكم والمعالجة، من أبرزها:

1. السرية: منع وصول غير المخولين للبيانات من خلال آليات التحكم في الوصول والمصادقة المتعددة العوامل.

2. الإبلاغ عن التسريب: إشعار الجهات المختصة وصاحب البيانات فور حدوث الاختراق.

وتشمل الالتزامات التقنية التفصيلية:

1. التشفير: يجب تشفير البيانات أثناء نقلها وتخزينها، خاصة البيانات الحساسة، باستخدام معايير تشفير قوية مثل AES-256.
2. النسخ الاحتياطية: إنشاء نسخ احتياطية مشفرة ومؤمنة لضمان استمرارية الخدمة واستعادة البيانات في حال حدوث اختراق.
3. مراجعة سجلات الدخول: تسجيل وتحليل جميع عمليات الدخول إلى أنظمة البيانات، مع الاحتفاظ بسجلات التدقيق لمدة كافية، لتمكين تتبع أي عملية غير مصرح بها.
4. مراقبة النشاطات المشبوهة: استخدام أنظمة كشف الاختراق (IDS) وأنظمة منع الاختراق (IPS)، وتفعيل التنبيهات الفورية لأي نشاط غير عادي.
5. تدريب الموظفين: توعية وتدريب جميع العاملين على مبادئ حماية البيانات وأمن المعلومات، وعلى كيفية التعامل مع حالات الاختراق المحتملة.
6. إدارة الثغرات: تحديث الأنظمة والبرامج باستمرار وسد الثغرات الأمنية المكتشفة، والاستجابة السريعة لأي تقارير عن ثغرات جديدة.
7. تقييم أثر حماية البيانات: إجراء تقييمات دورية لأثر المعالجة على خصوصية الأفراد (DPIA).

مدة الإبلاغ عن التسريب: تشترط اللائحة الأوروبية الإبلاغ خلال 72 ساعة من العلم بالاختراق. وتشير دراسة القرشي (2026) إلى أن معظم التطبيقات تحصل على موافقات "عشوائية" من المستخدمين لا تتوافق مع روح النظام، وتدعو سدايا إلى تكثيف الرقابة اللاحقة وفرض غرامات رادعة.¹³

الفصل الثاني: حقوق صاحب البيانات وآليات ممارستها

يحدد هذا الفصل الحقوق المقررة لأصحاب البيانات وآليات ممارستها، بما في ذلك الحق في العلم والوصول والحقوق التصحيحية والنهائية. وهذه الحقوق هي التي تمكن الفرد من السيطرة على معلوماته الشخصية، وممارسة ما يُعرف بـ "تقرير المصير المعلوماتي".

¹³ p 32 Smith, J., & Brown, L. (2019). Research methods in psychology. Sage Publications

المبحث الأول: الحق في العلم والوصول

يُعد الحق في العلم والوصول من الحقوق الأساسية التي تمكن صاحب البيانات من معرفة كيفية معالجة بياناته والاطلاع عليها. وهذا الحق هو الذي ينبثق منه باقي الحقوق، إذ لا يمكن للفرد أن يمارس حقه في التصحيح أو الإزالة إذا لم يكن يعلم أصلاً ما هي البيانات المحفوظ بها، ويمنح القانون صاحب البيانات الحق في معرفة من يجمع البيانات ولماذا، والحق في الوصول لنسخة البيانات بدون رسوم، وتشمل آليات الممارسة:

1. الإفصاح المسبق: يجب على جهة التحكم تزويد صاحب البيانات بإشعار واضح ومبسط قبل البدء بجمع بياناته، يتضمن جميع المعلومات الجوهرية عن المعالجة بلغة مفهومة للشخص العادي.
2. الرد على طلبات الوصول: يجب على جهة التحكم الرد على طلب الوصول خلال مهلة زمنية معقولة (30 يوماً في اللائحة الأوروبية)، وتزويد صاحب البيانات بنسخة من بياناته بصيغة إلكترونية مفهومة.
3. الاستثناءات: يجوز لجهة التحكم رفض طلب الوصول أو تقييده إذا كان من شأنه الإضرار بحقوق الآخرين أو بأمن الدولة، مع ضرورة تبرير الرفض كتابةً.
4. عدم التمييز: لا يجوز لجهة التحكم فرض رسوم على طلبات الوصول الأساسية، ولا التمييز ضد صاحب البيانات لمجرد ممارسته لحقوقه.
5. تقديم الشكاوى: يحق لصاحب البيانات تقديم شكوى إلى الهيئة الرقابية المختصة إذا لم تستجب جهة التحكم لطلبه، أو إذا اعتقد أن حقوقه قد انتهكت.

المبحث الثاني: الحقوق التصحيحية والنهائية (الحق في النسيان)

تتجاوز حقوق صاحب البيانات مجرد العلم والوصول لتشمل حقوقاً تصحيحية ونهائية تمكنه من التحكم الفعلي في بياناته. ويُعد "الحق في النسيان" من أحدث هذه الحقوق وأكثرها إثارة للجدل، إذ يتعارض أحياناً مع حقوق أخرى كحرية التعبير وحق الجمهور في المعرفة، ويمنح القانون صاحب البيانات مجموعة من الحقوق التصحيحية والنهائية، منها:

1. الحق في التصحيح: تعديل البيانات أو استكمال الناقصة، بحيث تعكس واقع الفرد بدقة.
2. الحق في الإزالة (النسيان): مسح البيانات عند انتهاء الغرض أو سحب الموافقة، أو عندما تصبح البيانات غير ضرورية للغرض الذي جمعت من أجله.
3. الحق في الاعتراض على المعالجة: يحق لصاحب البيانات الاعتراض في أي وقت على معالجة بياناته لأسباب تتعلق بوضعه الخاص، حتى لو كان الأساس القانوني للمعالجة هو المصلحة المشروعة لجهة التحكم.¹⁴

¹⁴Chambers and Partners. (2026). TMT 2026 - Saudi Arabia: Trends and Developments p56

4. الحق في نقل البيانات: وهو الحق في استلام بياناته بصيغة منظمة وشائعة الاستخدام (مثل CSV أو JSON) ، ونقلها إلى جهة أخرى. هذا الحق لم ينص عليه صراحة في النظام السعودي أو المصري بعد، مما يمثل فجوة تشريعية ينبغي معالجتها.
5. الحق في تقييد المعالجة: يحق للفرد تقييد معالجة بياناته في حالات معينة، مثل الطعن في دقة البيانات، أو عدم قانونية المعالجة، أو اعتراض الفرد على المعالجة.

يمكن تطبيق هذه الحقوق عملياً من خلال لوحات التحكم في حسابات المستخدمين على منصات التواصل الاجتماعي والتجارة الإلكترونية، حيث توفر معظم هذه المنصات الآن خيارات لتنزيل البيانات، وتعديلها، وطلب حذف الحساب.

الباب الثالث: المسؤولية القانونية عن انتهاك البيانات الشخصية

يتناول هذا الباب أركان المسؤولية التقصيرية عن الانتهاك الرقمي والجزاءات المقررة وآليات جبر الضرر الناشئ عن انتهاك البيانات الشخصية، فوجود الحقوق والالتزامات دون آليات لإنفاذها وتطبيقها يجعلها مجرد نصوص نظرية لا قيمة عملية لها.

الفصل الأول: أركان المسؤولية التقصيرية عن الانتهاك الرقمي

يقوم هذا الفصل بتحليل أركان المسؤولية التقصيرية الثلاثة (الخطأ والضرر وعلاقة السببية) في سياق انتهاك البيانات الشخصية في البيئة الرقمية، مبيناً الخصوصيات التي تميز هذه الأركان في البيئة الرقمية عن مثيلاتها في البيئة التقليدية.

المبحث الأول: الخطأ في معالجة البيانات

تهدف المسؤولية الجنائية والعقوبات النظامية إلى تحقيق الردع العام والخاص من خلال توقيع عقوبات رادعة على المخالفين لأحكام حماية البيانات الشخصية، وتتفاوت هذه العقوبات بين الأنظمة المختلفة من حيث النوع والشدة.¹⁵

تعد المسؤولية الجنائية الركيزة الأساسية لضمان احترام أحكام حماية البيانات الشخصية، إذ أن وجود عقوبات رادعة يشكل الحافز الأقوى للجهات والأفراد للامتثال للالتزامات القانونية. وتختلف طبيعة العقوبات بين الأنظمة الثلاثة محل الدراسة، حيث يمزج النظام السعودي بين العقوبات السالبة للحرية والغرامات المالية، بينما يعتمد القانون المصري نظاماً مشابهاً مع فروق في المبالغ، في حين تتبنى اللائحة الأوروبية نظاماً إدارياً بحتاً قائماً على الغرامات المالية الضخمة.

¹⁵ الرحيلي، رباب عبد الله. (2025) مرجع سابق ص53

أولاً: العقوبات في النظام السعودي

نص نظام حماية البيانات الشخصية السعودي الصادر بالمرسوم الملكي رقم (م/19) وتاريخ 1443/2/9هـ، والمعدل بالمرسوم الملكي رقم (م/148) وتاريخ 1444/9/5هـ، على عقوبات صارمة للمخالفات.

نصت المادة على أن كل من أفصح عن بيانات حساسة أو نشرها مخالفاً أحكام النظام يعاقب بالسجن مدة لا تزيد على سنتين وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين. وتشدّد العقوبة إذا كان الإفصاح بقصد الإضرار بصاحب البيانات أو بقصد تحقيق منفعة شخصية. كما نص النظام على أن كل من خالف أيّاً من أحكامه الأخرى يعاقب بالسجن مدة لا تزيد على سنة وبغرامة لا تزيد على مليون ريال، أو بإحدى هاتين العقوبتين.

إلى جانب العقوبات الأصلية، يشمل النظام عقوبات تكميلية تشمل مصادرة الأجهزة والوسائل المستخدمة في المخالفة، والتشهير بالحكم الصادر على نفقة المخالف، ومنع المخالف من ممارسة النشاط المرتبط بالبيانات لفترة محددة. كما أقر النظام مسؤولية الشخص الاعتباري (الشركات والمؤسسات) عن المخالفات التي ترتكب باسمها أو لحسابها، بالإضافة إلى مسؤولية المديرين التنفيذيين والموظفين المسؤولين عن المخالفة، ونص على إمكانية مضاعفة العقوبة في حالة العود، وأوكل مهمة التحقيق والادعاء أمام القضاء إلى النيابة العامة.¹⁶

ثانياً: العقوبات في القانون المصري

نص القانون المصري رقم 151 لسنة 2020 بشأن حماية البيانات الشخصية على عقوبات جنائية تهدف إلى حماية البيانات الشخصية وردع المخالفين.

يعاقب كل من أفصح عن بيانات شخصية أو نشرها أو أتاح الاطلاع عليها لغير ذي صفة دون سند قانوني بالحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تزيد على مليون جنيه، أو بإحدى هاتين العقوبتين. كما يعاقب كل من خالف أحكام القانون المتعلقة بمعالجة البيانات الشخصية، كعدم الحصول على موافقة صاحب البيانات أو معالجتها لغرض غير مصرح به، بالغرامة التي لا تقل عن عشرين ألف جنيه ولا تزيد على خمسمائة ألف جنيه، وتكون العقوبة مضاعفة في حالة مخالفة أحكام معالجة البيانات الحساسة.

نص القانون على مضاعفة الحد الأقصى للعقوبات المقررة في حالة العود خلال فترة زمنية محددة. وأسند المشرع المصري اختصاص نظر قضايا حماية البيانات الشخصية إلى المحاكم الاقتصادية، وهي محاكم متخصصة في القضايا التجارية والاقتصادية. وتشمل العقوبات الإضافية نشر الحكم على نفقة المخالف، وسحب الترخيص أو إيقاف النشاط في بعض الحالات، وإغلاق المنشأة أو الموقع الإلكتروني المخالف.

¹⁶ إسماعيل، أماني مشهور. (2024) ص 65

ثالثاً: العقوبات في اللائحة الأوروبية (GDPR)

تتبنى اللائحة العامة لحماية البيانات (GDPR) نظاماً إدارياً بحتاً للعقوبات، حيث تعتمد على الغرامات المالية كأداة ردع أساسية، دون تضمين عقوبات سالبة للحرية، وقد اختار المشرع الأوروبي هذا النهج لأن الغرامات المالية الضخمة أكثر فعالية في ردع الشركات والكيانات الاعتبارية من العقوبات السالبة للحرية.

تصل الغرامات الإدارية إلى 20 مليون يورو أو 4% من إجمالي حجم التداول العالمي السنوي للشركة، أيهما أكبر، وذلك في حالات المخالفات الجسيمة. أما المخالفات الأقل خطورة فتتراوح غراماتها بين 10 ملايين يورو أو 2% من حجم التداول السنوي. وقد أظهر تقرير DLA Piper السنوي أن السلطات الإشرافية الأوروبية أصدرت غرامات بلغ مجموعها حوالي 1.2 مليار يورو في عام 2025، ومنذ تطبيق اللائحة في مايو 2018 وحتى يناير 2026، بلغ إجمالي الغرامات المسجلة 7.1 مليار يورو.

تصدرت أيرلندا قائمة الدول من حيث قيمة الغرامات، حيث أصدرت هيئة حماية البيانات الأيرلندية غرامة قدرها 530 مليون يورو في أبريل 2025 ضد شركة وسائل تواصل اجتماعي (تيك توك) لخرقها قواعد نقل البيانات الدولية. كما أصدرت هيئة حماية البيانات الفرنسية (CNIL) غرامات بلغ مجموعها 486.8 مليون يورو في عام 2025.¹⁷

شهد عام 2025 زيادة ملحوظة بنسبة 22% في الإخطارات اليومية بانتهاكات البيانات الشخصية، لتصل إلى متوسط 443 إخطاراً في اليوم، وهي المرة الأولى منذ تطبيق اللائحة التي يتجاوز فيها متوسط الإخطارات اليومية 400. وتعدّ التقارير هذه الزيادة إلى التوترات الجيوسياسية، وزيادة الهجمات السيبرانية، وتوفير تقنيات جديدة يستغلها المهاجمون.

بالإضافة إلى الغرامات المالية، تمنح اللائحة الهيئات الرقابية صلاحية فرض عقوبات إضافية، مثل إصدار تحذيرات أو توبيخات، وفرض حظر مؤقت أو دائم على معالجة البيانات، وأمر بتصحيح البيانات أو حذفها أو تقييد معالجتها، وسحب الشهادة المعتمدة في مجال حماية البيانات.

رابعاً: التطورات الحديثة في الإنفاذ

شهدت فترة ما بعد عام 2025 تطورات مهمة في مجال إنفاذ قوانين حماية البيانات على المستويين السعودي والأوروبي.

في السعودية: أعلنت الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) في يناير 2026 أن لجانها المتخصصة أصدرت 48 قراراً رسمياً تؤكد مخالفات لنظام حماية البيانات الشخصية، وهو عدد كبير يعكس نشاطاً رقابياً مكثفاً، ويمثل تحولاً حاسماً من فترة السماح الأولية إلى مرحلة إنفاذ صارم، ويعد أول موجة كبرى من العقوبات المفروضة على مراقبي البيانات الذين فشلوا في الوفاء بالتزاماتهم القانونية.

¹⁷ DLA Piper. (2026). GDPR Fines and Data Breach Survey 2025. DLA Piper p 56

في أوروبا: استمرت وتيرة الإنفاذ العالية في عام 2026، حيث أصدرت السلطات الإشرافية الأوروبية غرامات بلغت 68.18 مليون يورو في الربع الأول من عام 2026، وهو ارتفاع كبير مقارنة بـ 13.8 مليون يورو في الربع الأول من عام 2025. كما بلغ إجمالي عدد الغرامات المسجلة حتى مارس 2026 حوالي 2,685 غرامة، بمتوسط غرامة قدره 2.27 مليون يورو.

دعاوى التعويض: إلى جانب الغرامات الإدارية، شهد عام 2025 زيادة في مخاطر دعاوى التعويض بموجب المادة 82 من اللائحة الأوروبية، خاصة فيما يتعلق بالأضرار غير المادية مثل الضيق أو القلق الناجم عن خروقات البيانات. وقد أوضحت المحاكم الأوروبية أن المدعين يمكنهم متابعة دعاوى للحصول على تعويضات عن الضيق العاطفي حتى في غياب ضرر مادي ملموس.

وتشير هذه التطورات إلى أن حماية البيانات الشخصية لم تعد مجرد التزام نظري، بل أصبحت واقعاً عملياً تفرضه عقوبات ملموسة، مما يستوجب على جميع الجهات المعنية تعزيز امتثالها للأنظمة ذات الصلة والاستثمار في التدابير الأمنية والتقنية التي تضمن حماية البيانات الشخصية وتجنب المخاطر القانونية والمالية المترتبة على المخالفات

المبحث الثاني: الضرر وعلاقة السببية في الفضاء الافتراضي

يكتسي الضرر الناشئ عن انتهاك البيانات الشخصية طابعاً خاصاً، كما تطرح علاقة السببية تحديات كبيرة في البيئة الرقمية. فالضرر في هذا المجال غالباً ما يكون معنوياً أكثر منه مادياً، مما يجعل تقديره صعباً.

- الضرر المادي: سرقة أرقام بطاقات، خسائر مالية، عمليات احتيال، وسرقة هوية.
- الضرر المعنوي: أذى نفسي، قلق، خوف، تشهير، فقدان سمعة، وإحراج اجتماعي.
- إشكالية السببية: صعوبة إثبات المسؤولية عند تعدد الأطراف، خاصة في البيئات السحابية المشتركة حيث تتداخل مسؤوليات المراقب والمعالج والمزود السحابي.¹⁸

وتشمل أنواع الضرر التفصيلية:

1. الضرر المادي المباشر: الخسائر المالية الناجمة عن سرقة الحسابات البنكية أو عمليات الشراء غير المصرح بها باستخدام البيانات المسروقة.
2. الضرر المادي غير المباشر: تكاليف استعادة الهوية، وتكاليف تغيير البطاقات والمستندات، وفقدان فرص العمل أو الترقيات بسبب تسريب معلومات شخصية.
3. الضرر المعنوي: الألم النفسي، والقلق، والخوف، والشعور بالتعري، وفقدان السمعة، والتشهير، والإحراج الاجتماعي.

¹⁸ رجب، هبة رمضان. (2024). مرجع سابق ص 45

4. الضرر المستقبلي: خطر التعرض للاحتيال مستقبلاً بسبب بقاء البيانات المسروقة متداولة في السوق السوداء الإلكترونية.

ولمواجهة إشكالية إثبات علاقة السببية، اقترح الفقه القانوني عدة حلول: تخفيف عبء الإثبات (قلب عبء الإثبات) بإلزام جهة التحكم بإثبات أنها اتخذت جميع التدابير المطلوبة، ونظرية السببية المحتملة التي تقبل الدليل على وجود احتمال قوي أن الضرر ناتج عن خطأ الجهة، والمسؤولية الموضوعية (المسؤولية المشددة) التي بدأت تجد طريقها إلى بعض التشريعات الأوروبية.

الفصل الثاني: الجزاءات المقررة وآليات جبر الضرر

يتناول هذا الفصل الجزاءات الجنائية والنظامية المقررة لانتهاك البيانات الشخصية، وكذلك آليات التعويض المدني وجبر الضرر، فالجانب الجزري هو الذي يكفل احترام القواعد القانونية، حيث أن وجود العقوبات يشكل رادعاً للمخالفين.

المبحث الأول: المسؤولية الجنائية والعقوبات النظامية

تختلف العقوبات المقررة لانتهاك البيانات الشخصية بين النظام السعودي والقانون المصري واللائحة الأوروبية من حيث طبيعتها وشدتها، مما يعكس اختلافاً في النهج التشريعي بين هذه الأنظمة.

في النظام السعودي: غرامات تصل 5 مليون ريال وسجن حتى سنتين، مصادرة أجهزة، تشهير. فقد نصت المادة على أن كل من أفصح عن بيانات حساسة أو نشرها مخالفاً أحكام النظام يعاقب بالسجن مدة لا تزيد على سنتين وبغرامة لا تزيد على ثلاثة ملايين ريال، أو بإحدى هاتين العقوبتين. وفي تطور لافت، أعلنت الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) في يناير 2026 أن لجانها المتخصصة أصدرت 48 قراراً رسمياً تؤكد مخالفات لنظام حماية البيانات الشخصية، وهو ما يمثل تحولاً من فترة السماح إلى مرحلة إنفاذ صارم.¹⁹

في القانون المصري: غرامات وحبس بحسب جسامة الجرم، مضاعفة العقوبة في حال العود. ونص القانون المصري على عقوبات تصل إلى الحبس مدة لا تقل عن ثلاثة أشهر ولا تزيد عن سنة، وبغرامة لا تقل عن 50 ألف جنيه ولا تزيد عن مليون جنيه. وأسند المشرع المصري اختصاص نظر قضايا حماية البيانات الشخصية إلى المحاكم الاقتصادية، وهي محاكم متخصصة في القضايا التجارية والاقتصادية.

¹⁹ الجبجكي، تمام عبداللطيف. (2025). ص 85

في اللائحة الأوروبية (GDPR) تفرض اللائحة الأوروبية غرامات إدارية ضخمة تصل إلى 20 مليون يورو أو 4% من إجمالي حجم التداول العالمي السنوي للشركة، أيهما أكبر. وفي عام 2025، أصدرت السلطات الإشرافية الأوروبية غرامات بلغ مجموعها حوالي 1.2 مليار يورو، وكانت أكبر غرامة 530 مليون يورو ضد شركة وسائل تواصل اجتماعي. كما لوحظ زيادة بنسبة 22% في الإخطارات اليومية بانتهاكات البيانات، مما يعكس تصاعداً في المخاطر السيبرانية.

المبحث الثاني: المسؤولية المدنية والتعويض

هدف المسؤولية المدنية إلى جبر الضرر الواقع على صاحب البيانات نتيجة انتهاك خصوصيته الرقمية، وتقوم على القواعد العامة للمسؤولية التقصيرية، مع خصوصيات تفرضها طبيعة البيئة الرقمية والضرر المعنوي الناشئ عن انتهاك البيانات الشخصية، تستند دعوى التعويض المدنية عن انتهاك البيانات الشخصية إلى القواعد العامة للمسؤولية التقصيرية في القانون المدني، وبالاستناد إلى القواعد العامة للمسؤولية المدنية بأركانها الثلاثة: الخطأ، والضرر، وعلاقة السببية، يمكن تقرير قيام المسؤولية المدنية عند الاعتداء على البيانات الشخصية، وتنص المادة 163 من القانون المدني المصري، والمادة 140 من النظام السعودي للقضاء، على أن كل من أحدث ضرراً للغير يلتزم بتعويضه، وهو ما ينطبق على حالات انتهاك البيانات الشخصية التي تسبب أضراراً مادية أو معنوية للأفراد.²⁰

وتتجلى أهمية المسؤولية المدنية في هذا المجال في كونها السبيل الوحيد لجبر الضرر الذي يصيب الفرد نتيجة انتهاك بياناته، خاصة في الحالات التي لا تتوفر فيها مسؤولية جنائية، أو عندما يكون الضرر المعنوي هو الأساس في الدعوى، إذ أن انتهاك الخصوصية الرقمية يُعد مساساً مباشراً بحقوق الشخصية يترتب عليه حق المتضرر في التعويض متى ثبت الاعتداء وما نتج عنه من ضرر معنوي أو نفسي أو معلوماتي، حتى في غياب ضرر مادي ملموس.

أولاً: أركان المسؤولية المدنية

الخطأ في معالجة البيانات: يتحقق الخطأ في معالجة البيانات بمخالفة الالتزامات القانونية المفروضة على جهات التحكم والمعالجة، سواء بفعل إيجابي أو سلبي. وتتمثل صور الخطأ في:

- **الخطأ الإيجابي:** معالجة غير مصرح بها للبيانات، أو استخدامها لغرض غير الذي جمعت من أجله، أو الإفصاح عنها لطرف ثالث دون سند قانوني، أو نقلها خارج الدولة بالمخالفة للضوابط.

²⁰ الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا). (2025) المبادئ التوجيهية لتقييم مخاطر نقل البيانات الشخصية إلى خارج المملكة.

• **الخطأ السلبي:** إهمال الإجراءات التقنية، كعدم تشفير البيانات، أو ترك ثغرات أمنية، أو عدم تدريب الموظفين.

مقياس الخطأ: يُقاس الخطأ بالمعيار المهني للشخص المتخصص أو الشركة التقنية، إذ لا يُطلب من جهة التحكم أن تكون محصنة ضد أي اختراق، بل أن تتخذ التدابير المعقولة والمتناسبة مع حجم المخاطر ونوع البيانات، وهو ما يُعرف بمعيار الشخص المعتاد في نفس الظروف.

الضرر الناشئ عن انتهاك البيانات: يُعد الضرر ركناً أساسياً في المسؤولية المدنية، ويتميز في مجال انتهاك البيانات الشخصية بكونه غالباً ما يكون معنوياً أكثر منه مادياً، مما يجعل تقديره وإثباته أكثر صعوبة. وتشمل أنواع الضرر:

- **الضرر المادي المباشر:** الخسائر المالية الناجمة عن سرقة الحسابات البنكية، أو إجراء عمليات شراء غير مصرح بها باستخدام البيانات المسروقة.
- **الضرر المادي غير المباشر:** تكاليف استعادة الهوية، وتكاليف تغيير البطاقات والمستندات، وفقدان فرص العمل أو الترقيات.
- **الضرر المعنوي:** الألم النفسي، والقلق، والخوف، والشعور بالتعري، وفقدان السمعة، والتشهير، والإحراج الاجتماعي.
- **الضرر المعلوماتي:** فقدان السيطرة على البيانات، وما يرتبط بذلك من تبعات اجتماعية ومهنية مستمرة.

ونثير مسألة الضرر المعنوي إشكاليات قانونية دقيقة، إذ أن القواعد التقليدية للمسؤولية المدنية لم تستوعب بشكل كافٍ الأضرار المستحدثة في البيئة الرقمية، ولا سيما الضرر المعنوي والضرر المعلوماتي، فضلاً عن صعوبات الإثبات وتقدير التعويض في بيئة تتسم بسرعة الانتشار وصعوبة محو الآثار الرقمية.²¹

علاقة السببية: تكمن الصعوبة في إثبات أن الاختراق حدث بسبب تقصير جهة التحكم تحديداً، لا بسبب خطأ من صاحب البيانات أو بسبب طرف ثالث مجهول، خاصة في البيئات السحابية المشتركة حيث تتداخل مسؤوليات عدة أطراف، ولمواجهة هذه الإشكالية، اقترح الفقه القانوني عدة حلول:

• **تخفيف عبء الإثبات (قلب عبء الإثبات):** إلزام جهة التحكم بإثبات أنها اتخذت جميع التدابير المطلوبة، وإلا اعتبرت مسؤولة.

²¹ الجيجكلي، تمام عبداللطيف. (2025). ص 54

• **نظرية السببية المحتملة:** قبول الدليل على وجود احتمال قوي أن الضرر ناتج عن خطأ الجهة، وليس اشتراط اليقين المطلق.

• **المسؤولية الموضوعية (المشددة):** إقرار مسؤولية جهة التحكم بمجرد وقوع الاختراق، دون حاجة لإثبات خطأ، وهو اتجاه بدأ يجد طريقه إلى بعض التشريعات الأوروبية والمقترحات الفقهية العربية.

ثانياً: آليات جبر الضرر والتعويض

دعوى التعويض: تستند دعوى التعويض المدنية إلى القواعد العامة للمسؤولية التقصيرية، ويتطلب الحصول على التعويض إثبات الأركان الثلاثة (الخطأ، الضرر، علاقة السببية)، وقد أتاح النظام السعودي لأصحاب البيانات المتضررين الحق في المطالبة بتعويضات عن الأضرار التي لحقت بهم نتيجة سوء معالجة بياناتهم. كما نصت المادة 82 من اللائحة الأوروبية (GDPR) على أن "لكل شخص عانى ضرراً مادياً أو معنوياً نتيجة لانتهاك هذه اللائحة الحق في الحصول على تعويض من المراقب أو المعالج عن الضرر الذي لحق به"، وتترك السلطة التقديرية للقاضي لتقدير التعويض العادل، وفقاً لعناصر عدة:

- **حجم الضرر المادي والمعنوي:** مقدار الخسائر المالية، وشدة الألم النفسي، ومدى تأثير التسريب على سمعة المتضرر.²²
- **جسامة الخطأ:** هل كان الخطأ متعمداً أم ناتجاً عن إهمال جسيم أم مجرد إهمال بسيط.
- **الاستفادة من الانتهاك:** مقدار الربح أو المنفعة التي حققتها جهة التحكم من الانتهاك، بحيث يُحكم عليها بدفع مبلغ يعادل هذه المنفعة أو يتجاوزها (مبدأ عدم الاستفادة من الخطأ)
- **ظروف المتضرر:** وضعه المادي والاجتماعي، ومدى تأثره بالانتهاك.

صور التعويض: لا يقتصر التعويض على الجانب المالي، بل يشمل صوراً متنوعة، منها:

- وقف الانتهاك وإزالة آثاره.
- التعويض المالي عن الأضرار المادية والمعنوية.
- التعويض عن الضرر المعلوماتي وفقدان السيطرة على البيانات.

وتشير التطورات الأخيرة إلى أن مخاطر دعاوى التعويض بموجب اللائحة الأوروبية في تزايد، خاصة فيما يتعلق بالأضرار غير المادية مثل الضيق أو القلق الناجم عن خروقات البيانات، وقد أوضحت المحاكم

²² الجعيد، صالح عوض منصور. (2025) ص 74

الأوروبية أن المدعين يمكنهم متابعة دعاوى للحصول على تعويضات عن الضيق العاطفي، حتى في غياب ضرر مادي ملموس.

إنشاء صناديق تعويض للضحايا مجهولي المصدر: نظراً لصعوبة تحديد مصدر الاختراق أو هوية المخترق في بعض الحالات (خاصة في الهجمات الإلكترونية التي تنطلق من دول أخرى أو تستخدم شبكات مجهولة)، يُقترح في الفقه القانوني إنشاء صناديق تعويض وطنية أو إقليمية، تمول من اشتراكات إلزامية تدفعها جهات التحكم الكبرى، على أن تُستخدم هذه الصناديق لتعويض المتضررين من الانتهاكات التي يعجزون عن إثبات مرتكبها أو استيفاء حقوقهم منه، وهذا النموذج مطبق بالفعل في بعض الدول الأوروبية في مجالات أخرى (كالتعويض عن جرائم العنف)، ويمكن استلزامه في مجال انتهاكات البيانات الشخصية.

الخاتمة والتوصيات

النتائج

1. البيانات امتداد للذات البشرية وحمايتها جزء من حماية حقوق الإنسان. حماية البيانات الشخصية ليست مجرد مسألة تقنية أو قانونية، بل هي حماية للكرامة الإنسانية والحق في الخصوصية.
2. السعودية ومصر اعتمدتا معايير مشابهة GDPR مع مراعاة الخصوصية الوطنية، مما يعكس توجهاً تشريعياً متقدماً نحو حماية البيانات في المنطقة العربية.
3. الجزاءات المالية أكثر استخداماً للردع مقارنة بالسجن، خاصة في النظام الأوروبي الذي يعتمد على الغرامات النسبية كأداة ردع أساسية.
4. شهد عام 2025 تحولاً مهماً في تطبيق نظام حماية البيانات الشخصية السعودي، حيث أصبح الامتثال مطلباً تنفيذياً فورياً وليس اعتباراً مستقبلياً، وأصبح جزءاً أساسياً من المفاوضات التجارية والتدقيق الداخلي والتقييمات التنظيمية.
5. أصدرت سدايا 48 قراراً رسمياً تؤكد مخالفات للنظام، مما يمثل بداية مرحلة إنفاذ صارم ويثبت جدية الجهات التنظيمية في تطبيق النظام.
6. أظهرت اللائحة الأوروبية (GDPR) مستوى ثابتاً من الإنفاذ في عام 2025، مع غرامات بلغ مجموعها حوالي 1.2 مليار يورو، مما يعكس فعالية النظام الأوروبي في تحقيق الردع.
7. شهدت أوروبا زيادة بنسبة 22% في الإخطارات اليومية بانتهاكات البيانات، مما يعكس تصاعداً في المخاطر السيبرانية وتعقيد المشهد الرقمي.

8. رغم تقدم النصوص التشريعية، لا تزال هناك فجوة كبيرة بين النص النظامي والتطبيق العملي، لا سيما في التزام المواقع والتطبيقات الرقمية بمتطلبات الشفافية والخصوصية بالتصميم.
9. قواعد الإثبات التقليدية غير كافية في مواجهة الأدلة الرقمية، مما يستوجب استحداث آليات إثبات خاصة، كقلب عبء الإثبات، أو اعتماد نظرية السببية المحتملة.
10. الطبيعة العابرة للحدود للبيانات الرقمية تجعل من الصعب تطبيق التشريعات الوطنية بشكل فعال، وتستوجب تعاوناً دولياً وقضائياً لمواجهة الجرائم الإلكترونية.

التوصيات

1. **تفعيل القضاء التقني المتخصص** : عقد برامج تدريبية مستمرة للقضاة وأعضاء النيابة والمحامين في مجال الجرائم الإلكترونية وحماية البيانات، لضمان سرعة الفصل في المنازعات وإلمامهم بأدوات الإثبات الرقمية والتقنيات الحديثة.
2. **نشر التوعية حول سياسات الخصوصية** : زيادة الوعي المجتمعي بحقوق أصحاب البيانات وآليات ممارستها، وبالمخاطر المرتبطة بانتهاك الخصوصية الرقمية، من خلال حملات توعية وإعلامية مستمرة.
3. **إنشاء صناديق تعويض للانتهاكات مجهولة المصدر** : إنشاء صناديق تعويض وطنية تمول من اشتراكات إلزامية تدفعها جهات التحكم الكبرى، لتعويض المتضررين من الانتهاكات التي يعجزون عن إثبات مرتكبها.
4. **اقتراح تشريعات مستقبلية لتغطية ثغرات جديدة في البيئة الرقمية** : مواكبة التطورات التقنية المتسارعة، وتعديل التشريعات بشكل دوري لسد الثغرات المستجدة، خاصة في مجالات الذكاء الاصطناعي والبيانات الضخمة.
5. **تعديل نظام العقوبات** : العمل على تعديل نظامي السعودية ومصر بحيث تُحتسب الغرامات المالية كنسبة مئوية من حجم التداول السنوي للشركة المخالفة، على غرار النظام الأوروبي، لضمان ردع الشركات الكبرى.
6. **تعزيز الرقابة** : تفعيل دور الهيئات الرقابية المستقلة ومنحها صلاحيات تحقيق واسعة (كالاطلاع على الخوادم وطلب المستندات وفرض غرامات فورية)، مع تزويدها بالكوادر الفنية والتقنية اللازمة.
7. **تحديد مهلة الإبلاغ** : تحديد مهلة زمنية قصوى للإبلاغ عن الاختراقات (72 ساعة) على غرار اللائحة الأوروبية، مع فرض عقوبات تدريجية على التأخير في الإبلاغ.
8. **إصدار أدلة تقنية ملزمة** : إصدار أدلة تحدد الحد الأدنى من معايير الأمن السيبراني (التشفير، المصادقة متعددة العوامل، إدارة الثغرات، الاحتفاظ بسجلات التدقيق) التي يجب على كل جهة معالجة الالتزام بها، على غرار المعايير الدولية مثل ISO 27701.

9. تعزيز التعاون الدولي: توقيع اتفاقيات تعاون قضائي وأمني عربي ودولي لمكافحة الجرائم العابرة للحدود، وتبادل الخبرات في مجال التحقيق الرقمي، مع اعتماد مبدأ المعاملة بالمثل في تنفيذ الأحكام.

10. إلزام سياسات الخصوصية المبسطة: إصدار تعليمات بإلزام جهات التحكم بتقديم ملخص سياسة الخصوصية في صفحة واحدة بلغة عربية مبسطة، مع وضع نماذج موحدة للموافقة، لضمان عدم التقاف الجهات على الموافقة الصريحة بكتابات قانونية معقدة.

11. إجراء تقييمات دورية: إجراء تقييمات دورية لأثر المعالجة على الخصوصية (DPIA) خاصة عند استخدام تقنيات جديدة كالذكاء الاصطناعي، وإلزام الجهات بتقديم تقارير سنوية للهيئات الرقابية عن ممارساتها.

12. وضع معايير موحدة للتعويض: وضع معايير تقديرية للتعويض عن الأضرار المعنوية والمستقبلية، بحيث تكون متنسقة ومتناسبة مع حجم الانتهاك وخطورته.

قائمة المصادر والمراجع

أولاً: التشريعات والأنظمة

1. نظام حماية البيانات الشخصية السعودي، الصادر بالمرسوم الملكي رقم (م/19) وتاريخ 1443/2/9هـ، والمعدل بالمرسوم الملكي رقم (م/148) وتاريخ 1444/9/5هـ.

2. اللائحة التنفيذية لنظام حماية البيانات الشخصية، الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا)

3. القانون المصري رقم 151 لسنة 2020، بشأن حماية البيانات الشخصية.

4. اللائحة العامة لحماية البيانات (GDPR)، البرلمان الأوروبي والمجلس، 2016.

ثانياً: الدراسات والأبحاث الأكاديمية

5. الصرايرة، تقوى فارس محمد، وحسن، حسام الدين محمود محمد. (2025). الطبيعة القانونية للمسؤولية عن انتهاكات البيانات الشخصية الإلكترونية والتعويض عنها. مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، العدد 92. مسترجع من...https://jlr.journals.ekb.eg/article_509048

6. الرحيلي، رباب عبد الله. (2025). حماية البيانات الشخصية في البيئة الرقمية: دراسة مقارنة بين التشريعات العربية والدولية. المجلة الأمريكية الدولية للعلوم الإنسانية والاجتماعية. مسترجع من...<https://iajphss.us/>

7. الجعيد، صالح عوض منصور. (2025). الحماية الجزائية لمعالجة البيانات الشخصية في النظام السعودي (دراسة مقارنة). (مجلة الأندلس للعلوم الإنسانية والاجتماعية، المجلد 12، العدد 114).

8. إسماعيل، أماني مشهور. (2024) دور القانون الدولي لحقوق الإنسان في حماية خصوصية الأفراد: حق أساسي في العصر الرقمي [رسالة ماجستير غير منشورة]. جامعة الشرق الأوسط، الأردن.
9. القرشي، محمد الحسين. (2026). الإطار النظامي لحماية البيانات الشخصية في المملكة العربية السعودية وأثره على التزامات الجهات التقنية. *المجلة الدولية للبحوث القانونية والاجتماعية*.
10. مدبولي، باسم محمد فاضل. (2024). المسؤولية التقصيرية عن معالجة البيانات الشخصية في البيئة الرقمية (دراسة مقارنة). *(المجلة الأردنية للقانون والعلوم السياسية)*.
11. الجيكل، تمام عبداللطيف. (2025). حماية البيانات الشخصية للشركات والمؤسسات والأفراد وفقاً للمعايير الدولية وأحكام القانون الدولي الخاص. *المجلة الدولية للعلوم والبحوث*.
12. رجب، هبة رمضان. (2024). الحماية القانونية للبيانات الشخصية في عصر التكنولوجيا الرقمية. *مجلة العلوم القانونية والاقتصادية، كلية الحقوق جامعة عين شمس*.

ثالثاً: التقارير والمبادئ التوجيهية

13. الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا). (2025) *المبادئ التوجيهية لتقييم مخاطر نقل البيانات الشخصية إلى خارج المملكة*.
14. DLA Piper. (2026). *GDPR Fines and Data Breach Survey 2025*. DLA Piper..
15. Chambers and Partners. (2026). *TMT 2026 - Saudi Arabia: Trends and Developments*.

رابعاً: المراجع الأجنبية

16. Court of Justice of the European Union. (2024). *Case C-687/21 - Recht auf Schadensersatz gemäß Art. 82 GDPR*.
17. Smith, J., & Brown, L. (2019). *Research methods in psychology*. Sage Publications.