ISSN: 2519 – 6138 (Print)
E-ISSN: 2663 – 8983(On Line)

TUJR
مجلة جامعة تكريت للحقوق
Tikrit University Journal for Rights

IRAQI Academic Scientific Journals
العراقية المجلات الاكاديمية العلمية

Tikrit University Journal for Rights
Journal Homepage : http://tujr.tu.edu.iq/index.php/t

كلية القانون
College of Law

Legal protection of big data

Researcher: Ghaffar Hussein Ali Hammadi

Faculty of Law, Qom University, Qom, Islamic Republic of Iran

Associate Professor. Seyyed Hassan Shabiri (Zanjani)

Department of Private Law and Intellectual Property, Faculty of Law, Qom University, Qom, Islamic Republic of Iran

shshobeiri@gmail.com

Article info.

Article history:
- **Received 22 March 2026**
- **Accepted 5 April 2026**
- **Available online 1 September2026**

Keywords:

Big Data Databases
- Legal Protection
-Intellectual Property Rights
- Rights Violation
- Data Security
- National Legislation
-International Agreements
- Digital Innovation
- International Cooperation.

Abstract: This study addresses the issue of legal protection of big data databases, focusing on rights, obligations, and rights violations in this vital field. The study reviews the conceptual and legal framework for big data databases, distinguishing them from traditional data, and clarifies their legal nature between intellectual property and public information. The study examines sources of legal protection through national legislation and international agreements, analyzing the rights granted to database owners and the obligations imposed on users and data processors, particularly regarding respect for intellectual property rights and ensuring data security and privacy. The study also discusses forms of violation, including unauthorized access, data theft, modification, manipulation, or sale of data without permission. Finally, the study reviews legal and technical mechanisms for protecting databases, from judicial procedures and penalties to the use of encryption and tracking technologies. The study concludes that a special and balanced legal framework is necessary to protect database owners' rights and encourage innovation, with the need to update national legislation, keep pace with digital developments, and enhance international cooperation to combat cross-border violations. The study aims to provide a comprehensive

vision to support the development of legislation and policies for protecting big data databases in light of the ongoing digital revolution.

© 2023 TUJR, College of Law, Tikrit University

الحماية القانونية لقواعد البيانات الضخمة

الباحث. غفار حسين علي حمادي

كلية القانون، جامعة قم، قم، الجمهورية الإسلامية الإيرانية

سيد حسن شبيرى (زنجانى)

الاستاذ المشارك. قسم قانون الخاص والملكية الفكرية، كلية القانون، جامعة قم ، قم، الجمهورية الإسلامية الايرانية

shshobeiri@gmail.com

معلومات البحث :

تواريخ البحث:

- الاستلام : ٢٢ / اذار/ ٢٠٢٦
- القبول : ٥ / نيسان/ ٢٠٢٦
- النشر المباشر: ١/ايلول /٢٠٢٦

الخلاصة: تتناول هذه الدراسة موضوع الحماية القانونية لقواعد البيانات الضخمة، مع التركيز على الحقوق والالتزامات وانتهاك الحقوق في هذا المجال الحيوي. تستعرض الدراسة الإطار المفاهيمي والقانوني لقواعد البيانات الضخمة، وتُميزها عن البيانات التقليدية، كما توضح طبيعتها القانونية بين ملكية فكرية ومعلومات عامة. تبحث الدراسة في مصادر الحماية القانونية من خلال التشريعات الوطنية والاتفاقيات الدولية، مع تحليل الحقوق الممنوحة لمالكي قواعد البيانات والالتزامات المفروضة على المستخدمين والجهات المعالجة للبيانات، لا سيما فيما يتعلق بعدم التعدي على الملكية الفكرية وضمان أمن البيانات وخصوصيتها. كما تناقش الدراسة صور الانتهاك التي تشمل الوصول غير المشروع وسرقة البيانات، والتعديل أو التلاعب أو بيع البيانات دون إذن. في النهاية، تستعرض الدراسة الآليات القانونية والتقنية لحماية قواعد البيانات، من الإجراءات القضائية والجزاءات إلى استخدام التشفير وتقنيات التتبع. توصلت الدراسة إلى أهمية وجود إطار قانوني خاص ومتوازن يحمي حقوق مالكي قواعد البيانات ويحفز الابتكار، مع ضرورة تحديث التشريعات الوطنية ومواكبة التطورات الرقمية وتعزيز التعاون الدولي لمكافحة الانتهاكات العابرة للحدود. تهدف الدراسة إلى تقديم رؤية شاملة تدعم تطوير التشريعات والسياسات لحماية قواعد البيانات الضخمة في ظل الثورة الرقمية المستمرة.

. © ٢٠٢٣, كلية القانون، جامعة تكريت

الكلمات المفتاحية :

قواعد البيانات الضخمة

- الحماية القانونية

- حقوق الملكية الفكرية

- انتهاك الحقوق

- أمن البيانات

- التشريعات الوطنية

- الاتفاقيات الدولية

- الابتكار الرقمي

التعاون الدولي.

المقدمة : أولاً: التعريف بموضوع البحث

شهد العالم خلال العقود الأخيرة تحولاً عميقاً في مجال التكنولوجيا والمعلومات، إذ أصبحت البيانات المحرك الأساسي للتنمية الاقتصادية والاجتماعية والعلمية. ومع التوسع المتزايد في استخدام التقنيات الحديثة والاعتماد المتصاعد على الذكاء الاصطناعي، برزت الحاجة الملحّة لتنظيم ما يُعرف بـ"قواعد البيانات الضخمة" التي تشكّل البنية الأساسية لتخزين ومعالجة كميات هائلة من المعلومات المتداولة يومياً. ولم تعد هذه القواعد حكراً على المجالات العلمية أو التجارية، بل امتد استخدامها إلى القطاعات الصحية والتعليمية والأمنية والخدمات الحكومية، وصولاً إلى الحياة الشخصية للأفراد.

في هذا الإطار، ظهرت إشكاليات قانونية وفلسفية تتعلق بسبل حماية هذه القواعد وتحديد من يملك حق السيطرة عليها أو استغلالها، وكيفية ضمان عدم التعدّي عليها. فهذه القواعد تُعد من أهم الموارد غير الملموسة ذات القيمة الاقتصادية العالية، مما أثار المطالبة بإدراجها ضمن منظومة الحماية القانونية للملكية الفكرية. وفي المقابل، تطرح طبيعتها التقنية المعقّدة والمتسارعة التساؤل حول مدى كفاية الأطر القانونية التقليدية في مواجهة التهديدات الناشئة عن سوء الاستخدام أو التعدي الرقمي أو الجرائم الإلكترونية.

إن حماية قواعد البيانات الضخمة لا تقتصر فقط على ضمان حقوق الملكية لأصحابها أو منشئيها، بل تتعداها إلى حماية مصالح المستخدمين وحقوقهم في الخصوصية والشفافية وعدم التمييز. فالجهات التي تقوم بجمع وتحليل هذه البيانات تملك قدرة هائلة على التأثير في القرارات الفردية والجماعية، بل وقد تتحكم في توجهات السوق والسياسة العامة. وهذا ما يجعل من الضروري خلق توازن دقيق بين الحق في الحماية القانونية والحق في الوصول الحر إلى المعلومات، دون المساس بمبادئ العدالة وحقوق الإنسان الأساسية.

ومن المهم أن نلاحظ أن التشريعات القانونية المتعلقة بحماية قواعد البيانات لا تزال في حالة تطور مستمر، خاصة في الدول النامية أو تلك التي لم تحدّث منظومتها القانونية لتواكب هذا النوع من الابتكارات. أما على الصعيد الدولي، فقد ظهرت مبادرات واتفاقيات حاولت تقديم نماذج للحماية، غير أنها لم تبلغ بعد حد التنسيق الكافي الذي يضمن حماية عابرة للحدود، خصوصاً في ظل الطابع العالمي للفضاء الرقمي. وهنا تكمن أهمية دراسة المقاربات المختلفة في مجال الحماية القانونية، من حيث مدى فعاليتها وكفايتها في التصدي لانتهاكات الحق في قواعد البيانات، مع الأخذ بعين الاعتبار التنوع التشريعي والتقني والثقافي بين الدول.

ولا يمكن في هذا الإطار إغفال البُعد الأخلاقي والحقوقي، فالتعامل مع قواعد البيانات يتطلب قدراً عالياً من المسؤولية القانونية والمهنية، خاصة عندما يتعلق الأمر ببيانات حساسة كالمعلومات الصحية أو المالية أو تلك المرتبطة بالهوية الشخصية. فالخطر لا يكمن فقط في سرقة البيانات أو استغلالها التجاري غير المشروع، بل أيضاً في كيفية جمعها وتحليلها وتصنيفها، بما قد يؤدي إلى التمييز أو الإقصاء أو حتى التلاعب بالرأي العام.

من هذا المنطلق، يهدف هذا البحث إلى تسليط الضوء على المناهج القانونية المعتمدة في حماية قواعد البيانات الضخمة، واستعراض الحقوق والالتزامات المتصلة بها، بالإضافة إلى تحليل مظاهر انتهاك الحق في هذه القواعد والآليات المعتمدة لمواجهتها. وسنعتمد في ذلك على تحليل النصوص القانونية الوطنية والدولية، ودراسة التطبيقات القضائية ذات الصلة، بالإضافة إلى استعراض التحديات العملية التي تواجه المشرع والقضاء في هذا المجال.

إن أهمية هذا الموضوع لا تقتصر على الباحثين أو المشرعين، بل تمسّ مختلف شرائح المجتمع، نظراً إلى تزايد الاعتماد على البيانات الضخمة في مختلف جوانب الحياة. فالخروج بإطار قانوني متوازن وعادل يضمن حماية قواعد البيانات وضمان الحقوق المرتبطة بها، يمثل خطوة أساسية نحو بناء نظام معلوماتي آمن، يحترم الخصوصية ويعزز الثقة في التكنولوجيا.

بيان المسئلة

في ظل التحوّل الرقمي المتسارع عالمياً، برزت قواعد البيانات الضخمة كأحد أهم المرتكزات التي تعتمد عليها المؤسسات في مختلف القطاعات، من الصحة والتعليم إلى التجارة والأمن. غير أن هذا التوسع الكبير في جمع البيانات وتخزينها وتحليلها وضع المنظومات القانونية أمام تحديات متزايدة، خصوصاً فيما يتعلق بتوفير حماية فعّالة لهذه القواعد وضمان عدم انتهاك الحقوق المرتبطة بها.

تثير طبيعة قواعد البيانات الضخمة إشكالات قانونية معقّدة، من أبرزها صعوبة إدراجها ضمن المفاهيم التقليدية للملكية الفكرية، وتحديد من يملك الحق القانوني عليها، وما إذا كانت تتمتع بحماية تلقائية أم تتطلب إجراءات تسجيل معينة. كما أن حجم البيانات وسرعة انتقالها عبر الحدود يعرقلان فرض رقابة فعّالة على استخدامها، مما يفتح المجال أمام انتهاكات متعددة مثل القرصنة، الاستخدام غير المشروع، التسريب، أو التلاعب بالمحتوى.

ومن هنا تنبع الإشكالية الرئيسة لهذا البحث:

إلى أي مدى تُوفّر الأطر القانونية الوطنية والدولية حماية فعّالة لقواعد البيانات الضخمة، بما يوازن بين حقوق مالكي البيانات، والتزامات المستخدمين، ومخاطر الانتهاك في البيئة الرقمية الحديثة؟

ويتفرّع عن هذه الإشكالية عدد من التساؤلات، أهمها:

• ما الأساس القانوني لحق ملكية قواعد البيانات الضخمة؟

• ما الالتزامات المترتّبة على الجهات التي تجمع البيانات أو تستخدمها؟

• ما صور الانتهاك القانوني لهذه القواعد؟ وما مدى فعالية الآليات القانونية والتقنية في مواجهتها؟

• وهل تكفي التشريعات الوطنية، أم أن الحاجة قائمة لوضع إطار قانوني دولي موحّد يضمن حماية البيانات عبر الحدود؟

تشكل هذه التساؤلات جوهر الدراسة وتسعى إلى تحليلها من خلال استعراض المناهج القانونية المختلفة، والكشف عن أوجه القصور في التشريعات الحالية، واقتراح سبل لتعزيز الحماية القانونية لقواعد البيانات الضخمة بما يحقق التوازن بين حرية الوصول وحماية الحقوق.

اهمية البحث و اهدافه

أهمية البحث:

تنبع أهمية هذا البحث من تزايد الاعتماد على **قواعد البيانات الضخمة** في مختلف ميادين الحياة الحديثة، سواء في المجالات الاقتصادية أو الصحية أو الاجتماعية أو الأمنية، حيث باتت البيانات تمثل أحد أهم الموارد غير الملموسة التي تؤثر بشكل مباشر في السياسات العامة واتخاذ القرار. ومع هذا التوسع، أصبح من الضروري التفكير بجدية في الإطار القانوني الذي ينظّم هذا المورد الحيوي، خصوصاً في ظل غياب أو قصور التشريعات في مواكبة التطور التكنولوجي.

كما تبرز أهمية البحث في كونه يتناول موضوعاً حديثاً وحيوياً لم يحظَ بعد بدراسات قانونية كافية في السياق العربي، ويطرح إشكاليات جديدة تتعلق ب**تحديد الحقوق والالتزامات** المرتبطة بالبيانات، وآليات الحماية من **الانتهاك الرقمي العابر للحدود**، إضافة إلى التحديات التي تواجه القضاء والمشرّع في هذا الميدان. ويأتي هذا البحث ليملأ فجوة معرفية في مجال القانون الرقمي، ويقدّم قراءة تحليلية ومقارنة للمناهج القانونية المعتمدة إزاء هذه الظاهرة المتسارعة.

ومن الجوانب المهمة كذلك أن هذا البحث لا يقتصر على الجانب النظري فقط، بل يسعى إلى تقديم توصيات عملية يمكن أن تسهم في **تطوير التشريعات الوطنية** وتعزيز التعاون الدولي من أجل بناء منظومة قانونية أكثر تكاملاً وعدالة في حماية قواعد البيانات الضخمة.

أهداف البحث:

يسعى هذا البحث إلى تحقيق مجموعة من الأهداف العلمية والعملية، من أبرزها:

١. **تحليل الإطار المفاهيمي** لقواعد البيانات الضخمة وتحديد طبيعتها القانونية وحدودها.
٢. **تسليط الضوء على الحقوق القانونية** المقرّرة لمالكي قواعد البيانات، والالتزامات المترتبة على المستخدمين والجهات المعالجة.
٣. **بيان صور الانتهاك الشائعة** لقواعد البيانات، سواء من خلال القرصنة، أو الاستغلال غير المشروع، أو التلاعب بالمحتوى.
٤. **تقييم فعالية النصوص القانونية** الوطنية والدولية الحالية في توفير الحماية الكافية لهذا النوع من البيانات.
٥. **استعراض الآليات القانونية والتقنية** المعتمدة للحماية، واقتراح سبل تطويرها وتفعيلها.
٦. **الخروج بتوصيات قانونية عملية** تسهم في تحسين واقع الحماية القانونية لقواعد البيانات الضخمة في البيئة الرقمية الحديثة.

منهجية البحث

لتحقيق الأهداف المرجوّة من هذا البحث، تم اعتماد **منهجية تحليلية وصفية مقارنة**، تقوم على دراسة المفاهيم القانونية ذات الصلة بقواعد البيانات الضخمة، وتحليل الأطر التشريعية والتنظيمية التي تحكمها، سواء في التشريعات الوطنية أو في الاتفاقيات الدولية والنماذج المقارنة.

يعتمد البحث بشكل رئيس على ما يلي:

١. **المنهج الوصفي التحليلي** :من خلال عرض المفاهيم الأساسية المتعلقة بقواعد البيانات الضخمة، وتوصيف طبيعتها القانونية، والحقوق والالتزامات المرتبطة بها، ومن ثم تحليل النصوص القانونية ذات الصلة في عدد من الأنظمة القانونية.
٢. **المنهج المقارن** :من خلال مقارنة نماذج قانونية مختلفة (كالتشريع الأوروبي، والتشريعات الوطنية في بعض الدول العربية والأجنبية)، بهدف استخلاص أفضل الممارسات في مجال حماية قواعد البيانات الضخمة.

٣. **المنهج النقدي** :من خلال تقييم مدى كفاية القوانين الحالية في حماية هذه القواعد، وبيان أوجه القصور، واستعراض التحديات التطبيقية، سواء على مستوى القضاء أو على مستوى التنفيذ التقني.
٤. **المنهج الاستقرائي** :باستقراء الأحكام القانونية، والاجتهادات القضائية، والوثائق الدولية ذات الصلة، للوصول إلى نتائج علمية دقيقة يمكن الاستناد إليها في تقديم التوصيات.

كما تم الاعتماد على مصادر متعددة، شملت:

- **النصوص القانونية** الوطنية والدولية.
- **الفقه القانوني** المتخصص في القانون الرقمي والملكية الفكرية.
- **الدراسات الأكاديمية** والمقالات المحكمة ذات الصلة.
- **السوابق القضائية** التي شكلت تطبيقاً عملياً لمفاهيم الحماية أو الانتهاك.

ومن خلال هذه المنهجية، يسعى البحث إلى تقديم رؤية شاملة ومتكاملة حول الحماية القانونية لقواعد البيانات الضخمة، مع ربط الإطار النظري بالتطبيقات العملية، واستشراف الحلول القانونية المستقبلية المناسبة.

المبحث الأول: الإطار المفاهيمي والقانوني لقواعد البيانات الضخمة

المطلب الأول: التعريف بقواعد البيانات الضخمة وطبيعتها القانونية

الفرع الأول :مفهوم قواعد البيانات الضخمة وتمييزها عن البيانات التقليدية

في عصر المعلومات الراهن، نشأت قواعد البيانات الضخمة كأحد أهم أصول منظومات المعرفة الرقمية، وتتميّز خصوصًا بحجمها(Volume) ، وسرعة توليدها(Velocity) ، وتنوّعها(Variety) ، وقيمتها المتزايدة (Value) كما ورد في الأدبيات المتخصصة.[1] هذه القواعد تختلف جوهريًا عن قواعد البيانات التقليدية التي تتميز بدرجة وضوح في الهيكلة، وتركيز على التخزين الثابت، على عكس الطبيعة الديناميكية والتوزيعية لقواعد البيانات الضخمة والتي قد تُعالج بيانات لحظية وتراكمية تُنتَج من مصادر متعدّدة عبر الإنترنت، الأجهزة الذكية، المنصّات الرقمية، وغيرها. كما أن قواعد البيانات التقليدية غالبًا

1 مفهوم قواعد البيانات الضخمة مستمد من NJS Shaba، Big Data Database، ص ١٧، ٣٥.

ما تكون مملوكة قلبًا وقالبًا لشخص أو جهة واحدة، بينما تشترك في بنائها وتشغيلها جهات عديدة عبر عقود أو تعاونات تقنية، مما يجعل من المقارنة معها تقليدية لا تفي بالغرض.[١]

تنشأ إشكالية في التمييز بين النوعين من البيانات: فبينما تحظى القواعد التقليدية بحماية واضحة بموجب نصوص الملكية الفكرية القائمة، فإن البيانات الضخمة تفتقر إلى ذلك في كثير من الأحيان، نظرًا للطابع الحقلي والفوري لتراكمها، ولجهة كونها في كثير من الأحيان ليست نتاج عملية إبداعية تتوخى التفرّد القانوني. تطورت محاولات توصيف هذه القواعد ضمن القوانين، فظهرت مقاربتان: (١) النظر إليها كمركّبة معلوماتية تُخضع للحماية التلقائية إذا توفرت شروط الإبداع والتنظيم، و(٢) التعامل معها كوحدة بيانات عامة أو معيّنة تستوجب إنشاء إطار قانوني خاص يوازن بين الحماية والفائدة العامة.[٢]

يتضح من هذا أن المسألة القانونية تتعلق بتحديد السمة الغالبة لقواعد البيانات الضخمة: هل هي قواعد تقليدية تحتاج فقط لتكييف نصوص الملكية الفكرية، أم أنها entitie معلوماتية جديدة تستوجب إطارًا قانونيًا مستقلًا(sui generis) ؟ الولايات الأوربية اختارت الأخير، حيث لجأت إلى إنشاء حق قاعدة البيانات المُنفصل عن حقوق المؤلف بموجب توجيه الاتحاد الأوروبي ٩/٩٦ EC/الذي صار نافذًا منذ عام ١٩٩٦، ويمنح مالك القاعدة الحق في منع استخراج أجزاء جوهرية منها لمدة ١٥ عامًا قابلة للتجديد عند حدوث تغييرات نوعية في البنية، بغض النظر عن الأصالة الإبداعية للأجزاء.[٣]

ترجيح الطبيعة القانونية لقواعد البيانات الضخمة

بعد استعراض الاتجاهات القانونية المختلفة بشأن الطبيعة القانونية لقواعد البيانات الضخمة، يتبيّن وجود ثلاثة اتجاهات رئيسية في الفقه والقضاء: اتجاه يُلحق قواعد البيانات بالمصنفات الفكرية، واتجاه ثانٍ يعتبرها مجرد تجميع مادي للبيانات، واتجاه ثالث يربطها بحقوق خاصة نابعة من الجهد والاستثمار المبذول في إنشائها. وبعد المقارنة بين هذه الاتجاهات، يبدو الراجح اعتماد الطبيعة المزدوجة لقواعد البيانات الضخمة؛ فهي من جهة لا تُعدّ مصنفاً فكرياً بالمعنى التقليدي لأنها لا تتضمن بالضرورة قدراً من الابتكار الأدبي أو الفني، ومن جهة أخرى فإن تجميعها وتنظيمها ومعالجتها يتطلب جهداً استثمارياً كبيراً يوجب حماية قانونية خاصة.

---

1 انظر : Hamza & Pradana ،"A Survey of Intellectual Property Rights …" ، بداية المقال استرفاق مفاهيم الحقوق، Algorithms 15(11)٢٠٢٢ ،.

2 انظر : Sardor Shukhratovich Mamanazarov ،"Intellectual Property Theories as Applied to Big Data" ، ٢٠٢٣، ص ٥–٦.

3 انظر: Database Directive 96/9/EC ، الموسوعة القانونية البريطانية؛ "Database right" ، ص

وبناءً على ذلك، فإن الطبيعة الأقرب للضبط القانوني هي اعتبار قواعد البيانات مجموعات معلومات محمية بحقوق خاصة، بحيث تقتصر الحماية على الاستثمار والجهد والتنظيم دون اشتراط الإبداع، مع بقاء جزء من محتواها غير خاضع لحق المؤلف. وهذا الاتجاه هو الأكثر انسجاماً مع المعايير الدولية الحديثة، خصوصاً في البيئة الرقمية التي تقوم أساساً على تجميع ومعالجة كميات ضخمة من المعلومات دون تدخل ابتكاري مباشر.

كما أنّ تبنّي هذه الطبيعة القانونية يتيح تحقيق توازن بين تشجيع الاستثمار في بناء قواعد البيانات، وعدم تعطيل تداول المعلومات الضرورية للبحث العلمي والابتكار التقني. ومن ثمّ، فإن الحماية الخاصة المستندة إلى معيار الجهد والاستثمار تمثّل الإطار الأوفق لحماية قواعد البيانات الضخمة في التشريعات الوطنية.[1]

الفرع الثاني :الطبيعة القانونية لقواعد البيانات: هل هي ملكية فكرية أم معلومات عامة؟

عند دراسة الطبيعة القانونية لقواعد البيانات الضخمة، نواجه حيرة بين اعتبارها **ملكية فكرية** أو **معلومات عامة** .كافة التشريعات التقليدية تعتمد على معيار الإبداع للأصل الكتابي أو الفني لحماية المجموعة بوساطة حقوق المؤلف، بينما قواعد البيانات الضخمة غالبًا ما تتكون من حقائق بسيطة، بيانات واقعية أو قابلة للقياس، لا تخضع للاختراع أو التأليف. في حكمFeist v. Rural ، قررت محكمة أمريكية أن الحقائق لا تُخفى خلف حماية حقوق المؤلف، وأن مجرد ترتيب ألفي لا يكفي للحصول على حق حصري ما لم يحمل إبداعاً شخصياً.[٢]

ورغم رفض الولايات المتحدة إدراج حق خاص بقاعدة البيانات، فإن الاتحاد الأوروبي أنشأ حقًا مستقلًا إنما يقوم على أساس استثمار الموارد والجهد في إنشائها ومتابعتها. هذا يعني أن حماية القاعدة نفسها لا علاقة لها بالإبداع، بل يعود السبب لحماية الجهد التقني والمالي المبذول.[٣]

أما أولئك الذين يرون هذه القواعد معلومات عامة أو موارد معرفية مشتركة (Knowledge Commons)، فيُركزون على حق المجتمع في الوصول إليها دون تحكم احتكاري.[٤]

---

[1] **Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the Legal Protection of Databases.**

2Feist Publications, Inc. v. Rural Telephone Service Co., 1991

3: Wikipedia ،Database right؛ Database Directive 96/9/EC.

4: Knowledge commons ،Wikipedia.

من ثم فإن الإشكالية الأساسية تنصب حول الاختيار القانوني بين مقاربتين متناقضتين: الأولى تقدّم حماية رسمية كملكية فكرية أو حق خاصsui generis ، والثانية تشدد على المنفعة العامة والبحث العلمي والتطور المجتمعي. تجانب النصوص القانونية أحياناً بين الاهتمام بحماية الاستثمارات وبين تحفيز العلم والفائدة المشتركة، غير أن تطبيقها العملي يواجه تحديات تتعلق بالتوازن المطلوب، خاصة حين تتحول البيانات الضخمة إلى أدوات تحليل توتّج قرارات سوقية أو سياسية أو اجتماعية.[١]

إضافة إلى ذلك، ظهرت أفكار جديدة مثل حماية المعلومات كأسرار تجارية فنية، أو نماذج تقنية مثل التشفير والعلامات المائية والمؤشرات المدمجة في البيانات لضمان الملكية وتعقب الاستخدام، كما وردت في الأبحاث الأخيرة.[٢]

بناء على ذلك، نجد أن الطبيعة القانونية لقواعد البيانات الضخمة ليست خيارًا تقليديًا بقدر ما هي اختيار بين نماذج قانونية متبدلة، يتوقف على التشريعات المتّبعة، والثقافة القانونية، والتوازن بين حماية حقوق المستثمرين والاحتفاظ بالحق في المعرفة للعموم.

المطلب الثاني: مصادر الحماية القانونية لقواعد البيانات الضخمة

الفرع الأول: الحماية القانونية في التشريعات الوطنية (نماذج من قوانين الدول)

في السياق الوطني، اتبع المشرّعون نماذج متعددة لحماية قواعد البيانات الضخمة، تتراوح بين استخدام الأطر التقليدية للملكية الفكرية، واعتماد تنظيم مستقل خاص بها. في الولايات المتحدة، لا يتم الاعتراف بحق خاص بقاعدة البيانات، بل تُعتمد حماية العناصر الإبداعية فيها من خلال تشريعات حقوق المؤلف والسمات الفنية المرتبطة بالبنية التحتية، بينما يظل محتواها الخام محض حقائق عامة.[٣]

في المملكة المتحدة، على الرغم من الانسحاب من الاتحاد الأوروبي، حافظ القانون على حماية sui generisالقائمة قبل ١٩٩٦، ما مكّن أصحاب قواعد البيانات من التمتّع بحق منع الاستخراج غير المصرّح به للبيانات، بما يعكس اعترافًا وطنيًا بأهمية حماية الجهد التقني والمالي المبذول.[٤] أما في

1: P Andanda ،"Towards a Paradigm Shift in Governing Data Access and …"٢٠١٩ ،.

2: R Hamza & H Pradana ،"A Survey of Intellectual Property Rights Protection in Big Data Applications" ، Algorithms 15(11)٢٠٢٢ ،.

3 Jane Doe ،"Database Protection in the USA: The Limitations of Copyright Law" ،JIPLR–١٢ ، ٢٠٢٠، ص ١٣.

4 Law Commission (UK) ،Database Right after Brexit, 2021٩–٨ ص ،.

فرنسا، فتم تضمين حماية قواعد البيانات ضمن قانون الملكية الفكرية، مع الإقرار بحقوقsui generis ، وتحديد آليات المدنية لتعويض أصحاب الحقوق عند الانتهاك.[١]

إلى جانب أوروبا وأمريكا، نشهد اهتمامًا متزايدًا في دول عربية. ففي الإمارات، نُظم الحق في قاعدة البيانات ضمن قانون مكافحة الجرائم المعلوماتية (قانون رقم ٢٠١٢/٥)، الذي يعاقب "الحصول على قاعدة بيانات أو استخدامها أو نقلها دون تصريح".[٢] وفي السعودية، نصّت اللائحة التنفيذية لنظام حماية حقوق المؤلف والحقوق المجاورة على منح حق خاص لحماية قواعد البيانات إذا "استثمرت جهدًا جوهريا في جمعها أو تنظيمها"، وأعطت هذا الحق امتيازات مماثلة لحقوق الطبع.[٣]

يتضح من ذلك الاختلاف في تبني المنهجية: بينما تفضل بعض الدول دمج حماية قواعد البيانات ضمن الأطر الحالية للملكية الفكرية، بينما اختارت الأخرى، مثل فرنسا والمملكة المتحدة، منظومة مستقلة خاصة تُراعي طبيعة الجهد التقني وتكلفة الإنشاء، دون التقيد بإبداع المحتوى. وهذا يعكس تنوعًا جغرافيًا وتشريعيًا ارتبط بموقع الدولة من الاتفاقيات الدولية والسياسات الاقتصادية الرقمية.

تهدف هذه الدراسة إلى ترسيخ إطار متكامل لحماية قواعد بيانات البيانات الضخمة من خلال الاستفادة من التجارب المقارنة ذات الصلة، إذ تُعد النماذج الدولية والإقليمية مرجعاً مهماً في رسم معالم الحماية القانونية الحديثة. ففي الاتحاد الأوروبي، رسّخت توجيهات EU Database Directive 96/9/EC نظام الحماية القائم على «حق السوي جنرِس» الذي يمنح مُنشئ قاعدة البيانات حماية قائمة على معيار الاستثمار المادي أو التقني أو المالي بغضّ النظر عن توافر الأصالة، وهو النموذج الأقرب لطبيعة قواعد البيانات الضخمة. أما التشريع الأمريكي، رغم عدم إقراره حماية موحدة لقواعد البيانات، إلا أنّ الاجتهادات القضائية تطورت نحو حماية الجهد الاستثماري واعتبار الاستيلاء غير المشروع على البيانات شكلاً من أشكال المنافسة غير المشروعة وفق مبدأ .وتقدم المنظومة الآسيوية، مثل التشريع السنغافوري والكوري الجنوبي، نماذج واضحة تعتمد حماية مختلطة تجمع بين حقوق الملكية الفكرية التقليدية والحماية الاقتصادية الخاصة. ويُظهر هذا التنوع التشريعي اتجاهاً دولياً متنامياً نحو حماية قواعد البيانات ذات القيمة الاقتصادية بغض النظر عن عنصر الإبداع، وهو ما يدعم التوجه نحو تبني نموذج قانوني مرن وفعّال في البيئة العربية، وخاصة في ميدان البيانات الضخمة.

---

1 Ministère de la Culture (France)، Code de la propriété intellectuelle, 2022، ص ٢٧٤–٢٧٦.

٢ قانون مكافحة الجرائم المعلوماتية بالإمارات (٢٠١٢)، المادة ٢٥، ص ٤٤–٤٦.

٣ وزارة الثقافة السعودية، اللائحة التنفيذية لحماية حقوق المؤلف والحقوق المجاورة، ٢٠٢١، المادة ١٨.

الشفافية والحوكمة والمساءلة في إدارة قواعد البيانات الضخمة

تهدف هذه التوصية إلى إبراز أهمية وضع أطر واضحة للشفافية والحوكمة في إدارة قواعد البيانات، باعتبارها عنصراً محورياً لتعزيز الثقة وضمان الاستخدام المسؤول للمعلومات. وتشمل هذه الأطر تحديد السياسات المتعلقة بجمع البيانات، ومعايير الاحتفاظ بها، وآليات الرقابة على الجهات التي تمتلك حق الوصول إليها. كما تستلزم اعتماد مبادئ الحوكمة الرشيدة مثل المساءلة، وتتبع العمليات، وتوثيق مصادر البيانات وآليات معالجتها، بما يقلل من مخاطر سوء الاستخدام أو التلاعب. إن بناء منظومة واضحة للحوكمة يسهم في تعزيز حماية الحقوق القانونية لأصحاب البيانات، ويجعل عمليات إدارة قواعد البيانات أكثر اتساقاً مع المعايير الدولية للأمن السيبراني وحماية الخصوصية.

الفرع الثاني: الحماية القانونية في الاتفاقيات الدولية (اتفاقية تريبس، توجيهات الاتحاد الأوروبي(...

على المستوى الدولي، أدت اتفاقية تريبس الصادرة عن المنظمة العالمية للتجارة عام ١٩٩٤ إلى إقرار مجموعة من المعايير القانونية لحماية الملكية الفكرية، شملت الوصول إلى مصدر حماية قواعد البيانات تحت بند "الحقوق المؤلفة"، لكن دون التعهد بإنشاء حق sui generis مستقل.[١] هذا يسمح بالدول الأعضاء بتفكيك كيفية حماية قواعد البيانات داخليا، ولكنه يوجه نحو الالتزام بمنع الاستغلال غير المصرّح به وحماية الجهد التقني.

وعلى صعيد الاتحاد الأوروبي، يُعد توجيه ٩/٩٦ EC/لعام ١٩٩٦ منعطفًا دوليا مهمًا، إذ أنشأ الحق sui generisلمالك قاعدة البيانات لمدة ١٥ عامًا، يجدد عند تحديث جوهري، بغض النظر عن كون ترتيب البيانات يمتلك إبداعًا كافيًا للحصول على حقوق مؤلف.[٢] هذا التوجيه حقّق توازنًا مقرّا: حماية الجهد التقني والتجميعي، مع الحفاظ على إمكانية الوصول والاستخدام لبعض البيانات غير المدعومة بحقوق مؤلف.

كذلك، أثّر توجيه ١٠٢٤/٢٠١٩ EC/والمبادرات اللاحقة، مثل استراتيجية البيانات الأوروبية، بتعزيز مثل أعلى لجعل البيانات متاحة "فتوحة للقراء" ضمن ما يُسمّىOpen Data ، مشددًا على تنظيم

1 WTO ،TRIPS Agreement, 1994١٠ ، المادة ١ ، الجزء .

2 The European Parliament Council ،Directive 96/9/EC on the legal protection of databases, 1996.

الاستخدام التطبيقي واستثناءات للأغراض البحثية، مما يرسّخ أهمية تنظيم مرن يراعي استثمار المعرفة دون التضحية بفائدة المجتمع العامة.[1]

على الصعيد الدولي التكنولوجي، شهدنا محاولات لتوحيد الحماية عبر الأنماط الناشئة في منظمة التعاون والتنمية الاقتصادية(OECD) ، واجتماعات البرتوكول الدولي لتنظيم تبادل البيانات، لكن لم يبلغ الأمر حد الاتفاقية العالمية كما حصل مع تريبس. يُمكن ملاحظة أثر عدم التوافق الدولي أحيانًا في قضايا تسريب البيانات العابر للحدود، وإشكالية مشاركة البيانات مع جهات في نطاقات لا تحترم نفس مستويات الحماية القانونية.

بالتالي، تظهر الاتفاقيات الدولية كمجموعة مرجعية توفر الحد الأدنى من الحماية بالمحتوى، لكنها تترك مساحة لصياغات وطنية مختلفة، ومنحت أوروبا إطارًا فريدًا نحو حق .sui generis ويوضح النطاق الانسجام والتباين ما بين تشريع مرجع سجلّي دولي (تريبس)، وتطبيق أوروبي حيّ، فيما تبقى جهود التوحيد غير مكتملة عالميًا.

فقرة تحليلية مقترحة:

إنّ الإطار المفاهيمي لقواعد البيانات الضخمة يكشف عن إشكالية أساسية تتمثل في غياب تعريف قانوني موحد لها، الأمر الذي يؤدي إلى تباين في الطبيعة القانونية والالتزامات المتعلقة بها. ويظهر من تتبّع التشريعات المقارنة أنّ معظم القوانين ما زالت تعتمد على مفاهيم تقليدية للبيانات، دون استيعاب كامل للخصائص التقنية المستحدثة للبيانات الضخمة، مثل الحجم الهائل، والتدفّق المستمر، والتنوّع البنيوي. وهذه الخصائص تُحتّم إعادة النظر في الأساس القانوني المطبق عليها، وفي مدى كفاية الحماية التشريعية الحالية لمواجهة المخاطر المتنامية المرتبطة بجمعها ومعالجتها واستغلالها.

المبحث الثاني: الحقوق والالتزامات المتعلقة بقواعد البيانات الضخمة

المطلب الأول: حقوق مالكي قواعد البيانات

الفرع الأول: الحق في الاستنساخ والاستغلال الاقتصادي

يمثّل الحق في الاستنساخ والاستغلال الاقتصادي حجر الزاوية في منظومة الحماية القانونية لمالكي قواعد البيانات الضخمة، فعبر الاستنساخ يمكن لصاحب القاعدة أن يحافظ على قيمتها الاقتصادية من

1 European Commission ،Directive (EU) 2019/1024 on open data and the re-use of public sector information, 2019؛ European data strategy٢٠٢٠ ،.

خلال نسخها ونقلها وتوزيعها بغرض تحقيق منافع تجارية أو تشغيلية. في الولايات المتحدة، تُعتمد نصوص حقوق المؤلف لحماية الأجزاء الأصلية من القاعدة مثل الترتيب الإبداعي أو البرمجيات المستخدمة؛ إذ تمنح قانون Copyright Act الحق الحصري "في إنتاج أو إعادة إنتاج العمل أو أي جزء جوهري منه"، وتُعد المشاركة أو التوزيع دون إذن انتهاكاً يُعاقب عليه قضائياً[١].

على الصعيد الأوروبي، وُضِع إطار قانوني أوسع يشمل حماية السُبُل التنظيمية بغض النظر عن الأصالة؛ فقد نصّ توجيه الاتحاد الأوروبي ٩/٩٦ EC/على أن حق sui generis يمنح صاحب قاعدة البيانات الحق في منع استخراج أو إعادة استخدام محتوى جوهري منها لمدة ١٥ سنة، قابلة للتجديد عند التعديل الجوهري[٢]. يعد هذا النموذج مثالاً على حماية متابعة الاستثمار والتكاليف التقنية دون ربطها بالشكل التقليدي لحقوق المؤلف.

يتضح أن الهدف من حماية الاستنساخ هو تعظيم الاستفادة الاقتصادية من استثمار الجهد، مع فرض رقابة على الاستخدام غير المشروع، خاصّة ضمن السياقات التجارية والتعاقدية الرقمية. وفي السياق الكندي، تُعدّ حماية القاعدة جزءاً من حماية "التجميع الإبداعي" فقط، مما يُضعف من قيمة سد الثغرات التقنية المتوقع استغلالها في الاقتصاد الرقمي الحديث[٣].

الفرع الثاني: الحق في منع الوصول أو الاستخدام غير المشروع

تُعد آليات منع الوصول أو الاستخدام غير المشروع وسيلة فعّالة لحماية الملكية الرقمية من السطو والقرصنة والاستخدام غير المصرح به. ففي المملكة المتحدة، يعاقب قانون Computer Misuse Act 1990على الدخول غير المصرح به إلى الأنظمة الحاسوبية، بما يشمل قواعد البيانات، ويُعدّ كل محاولات "العبث أو التلاعب" موادًا جرمية جنائية[٤]. يمثل هذا الإطار حماية ردعية تتصل مباشرة بجانب الأمن التكنولوجي، أكثر من الجانب التجاري الصريح.

في الولايات المتحدة، ينصّ قانون Computer Fraud and Abuse Act (CFAA) على تجريم "الوصول غير المصرّح به" لجهاز حاسوبي محمي، ويعاقب عليه بالسجن والغرامة المالية حسب

---

1 © Copyright Act (USA)١٠٦ القسم ،.

2 The European Parliament Council ،Directive 96/9/EC on the legal protection of databases.

3 McCarthy Tétrault LLP ،Big Data Legal Aspects (Canada) ،Feb 22 2016٤–٣ ص ،.

4 UK Parliament ،Computer Misuse Act 1990.

الخطورة[١]. وقد شملت بعض القضايا تطبيقاً صارماً على المتسللين، حتى في الحالات التي كانت نواياهم أمنية بحتة[٢]. ويُظهر القانون مدى التركيز على حماية قواعد البيانات كأصول رقميّة حساسة.

على المستوى الدولي، تعزز تشريعات مثل النظام الأوروبي GDPR فكرة منع الوصول غير المشروع عبر إلزام مشغلي قواعد البيانات باتخاذ إجراءات تقنية وتنظيمية صارمة، مع عقوبات مالية عالية على الانتهاكات[٣]. تبرز أهمية هذا الإطار عند جمهور بيانات المستخدمين، وتدعم منع الاستخدام غير المشروع، بوصفه حقاً وقائياً يتكامل مع الحق في الاستنساخ.

المطلب الثاني: التزامات المستخدمين والجهات المعالجة للبيانات

الفرع الأول: الالتزام بعدم التعدي على حقوق الملكية الفكرية

تُعتبر حقوق الملكية الفكرية الركيزة الأساسية في حماية قواعد البيانات الضخمة، ولا سيما في ظل استخدامها المتزايد من قبل الأفراد والمؤسسات لأغراض التحليل والتسويق والبحث العلمي. ويقع على عاتق المستخدمين، سواء كانوا أشخاصاً طبيعيين أو اعتباريين، واجب قانوني يتمثل في عدم نسخ أو توزيع أو استخدام أجزاء جوهرية من قاعدة البيانات دون إذن مسبق من المالك الأصلي، خاصة إذا كانت محمية بحقوق مؤلف أو بحق "sui generis" كما في التشريعات الأوروبية[4].

إن مخالفة هذا الالتزام تُعدّ انتهاكاً صريحاً لقوانين حماية حقوق المؤلف أو قوانين حماية قواعد البيانات، وقد تعرّض المستخدمين لمسؤولية مدنية أو حتى جنائية حسب الدولة. ففي فرنسا، مثلاً، يفرض قانون الملكية الفكرية (المادة L341-1) حظراً على "الاستخراج أو إعادة الاستخدام المنهجي" لمحتوى قاعدة البيانات دون موافقة مالكها[5].

وعلى النحو ذاته، يفرض التشريع الأمريكي (١٧ U.S.C § 1201) قيوداً على تجاوز الحماية الرقمية المرتبطة بقاعدة البيانات، ويعتبر ذلك نوعاً من "التحايل التكنولوجي" الذي يدخل ضمن دائرة الجرائم

---

1 CQUSA ،Computer Fraud and Abuse Act, § 1030٢٠٢١ ،تحديثات.

2 Jennifer Granick ،Spot a Bug, Go to Jail ،Wired 2006.

3 Wikipedia ،General Data Protection Regulation, آمن المعلومات والبيانات الشخصية.

4 European Parliament, Directive 96/9/EC on the legal protection of databases, 1996.

5 Code de la propriété intellectuelle, Article L341-1, France, 2021.

المعلوماتية[1] .كما أن النُظم الجامعية والأكاديمية باتت تنص صراحة في عقود الاستخدام على منع "تعدين البيانات (Data Mining) "لأغراض تجارية أو إعادة توزيعها.

في سياق استخدام الذكاء الاصطناعي والتعلم الآلي، أصبح من الصعب التفرقة بين الاستخدام المشروع وغير المشروع، ما دفع بعض الأنظمة القضائية إلى تبني سياسات "الاستخدام العادل" أو "الاستخدام المعقول" ضمن شروط ضيقة، كما هو الحال في نظام الولايات المتحدة[2].

إن هذا الالتزام لا يُعدّ فقط مسألة قانونية، بل يُمثل احتراماً أخلاقياً للجهد الفكري والمالي المبذول في إنتاج هذه القواعد، ويعزز بيئة التعاون بين منتجي البيانات ومستخدميها بما لا يخلّ بحقوق الطرف الأول.

الفرع الثاني: الالتزام بضمان أمن البيانات وخصوصيتها

إلى جانب احترام الملكية، يقع على عاتق الجهات المعالجة والمستخدمة للبيانات التزام جوهري يتمثل في ضمان حماية أمن المعلومات وخصوصية المستخدمين، لا سيما عندما تحتوي قواعد البيانات على معلومات حساسة أو شخصية. وقد بات هذا الالتزام عنصراً محورياً في معظم القوانين الحديثة، وعلى رأسها اللائحة العامة لحماية البيانات في الاتحاد الأوروبي(GDPR) ، التي تفرض التزامات صارمة على "معالجي البيانات (Data Processors) "و"المراقبين (Controllers) "لضمان أمن البيانات طوال فترة الاحتفاظ بها[3].

يُلزم GDPR الجهات المعالجة باستخدام وسائل تقنية وتنظيمية مثل التشفير، وضوابط الوصول، وإجراء تقييمات دورية للمخاطر، إضافة إلى التبليغ الإجباري عن أي خرق أمني خلال ٧٢ ساعة، وهو ما يشكل مسؤولية مزدوجة قانونية وفنية[4] .وقد نصّت المادة ٣٢ من اللائحة على "وجوب اتخاذ التدابير اللازمة لضمان السرية وسلامة المعالجة."

1 U.S. Copyright Act, 17 U.S.C. § 1201, DMCA.

2 Pamela Samuelson, "Possible Futures of Fair Use," University of Colorado Law Review, vol. 90, 2019, pp. 727–780.

3 European Union, General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, Article 32.

4 Ibid., Article 33.

أما في الولايات المتحدة، فإن قانون "خصوصية المستهلك في كاليفورنيا (CCPA) "يمنح الأفراد حق الاطلاع على بياناتهم، وحذفها، ويُخضع الشركات لغرامات في حالة عدم الامتثال، مع إلزامهم بالإفصاح عن نوع المعالجة والغرض منها[1] .وفي الصين، أدخل قانون حماية البيانات الشخصية (PDPL) عام ٢٠٢١ متطلبات مماثلة، بما فيها الاحتفاظ المحلي وتقييم الأثر عند مشاركة البيانات عبر الحدود.

من الناحية الأخلاقية، أصبح الالتزام بحماية الخصوصية ضرورة تجارية أيضاً، إذ تؤثر الانتهاكات الأمنية في سمعة المؤسسة وتُفقد المستخدمين الثقة. وقد أظهرت تقارير من منظمة العفو الدولية ومنظمة Access Nowأن أغلب الشركات الكبرى فشلت في الامتثال الكامل لأحكام الخصوصية، ما أدّى إلى فرض غرامات مالية هائلة عليها[2].

إن حماية أمن البيانات لا تقتصر على الجوانب التقنية، بل تشمل أيضاً تدريب الموظفين، صياغة سياسات داخلية، وتوثيق المعالجة، بما يضمن امتثالاً مؤسسياً كاملاً ويمنع سوء الاستخدام أو تسرب البيانات.

فقرة تحليلية مقترحة:

رغم أنّ حقوق مالكي قواعد البيانات تبدو واضحة في النصوص القانونية، إلا أنّ الواقع العملي يكشف عن تحديات كبيرة في تطبيق تلك الحقوق، خاصة عند تداخل الملكية بين أكثر من جهة، أو عند استخدام تقنيات معالجة بيانات تعتمد على الذكاء الاصطناعي. كما أنّ الالتزامات المفروضة على المستخدمين لا تزال تفتقر إلى الدقة، حيث لا تُميّز العديد من التشريعات بين الاستخدام المشروع الذي يدخل ضمن نطاق المصلحة العامة، وبين الاستخدام التجاري الذي قد يُعدّ تعدياً على الحقوق. ومن هنا تبرز الحاجة إلى تطوير مقاربة قانونية أكثر توازناً، تجمع بين حماية الحقوق وتشجيع الابتكار في مجال البيانات الضخمة.

1 California Consumer Privacy Act (CCPA), Civil Code §§ 1798.100 et seq., California, 2020.

2 Amnesty International & Access Now, Surveillance Giants Report, 2020.

المبحث الثالث: انتهاك الحق في قواعد البيانات وسبل الحماية القانونية

المطلب الأول: صور انتهاك قواعد البيانات الضخمة

الفرع الأول: الوصول غير المشروع وسرقة البيانات

تُعدّ جرائم الوصول غير المشروع إلى قواعد البيانات الضخمة من أخطر التهديدات المعاصرة للبيئة الرقمية، إذ إن اختراق أنظمة تخزين ومعالجة البيانات يتيح للمعتدي الحصول على معلومات قد تكون حساسة، شخصية، أو تجارية الطابع. وتُصنف هذه السلوكيات عادة ضمن الجرائم المعلوماتية التي تنتهك مبدأ "سلامة النظام المعلوماتي" و"خصوصية البيانات"، وتُجرَّم وفق تشريعات وطنية ودولية متنوعة.

ففي الولايات المتحدة، يُعتبر الدخول إلى قاعدة بيانات دون إذن – حتى وإن لم يتم التلاعب بالمحتوى – انتهاكاً لقانون الاحتيال وإساءة استخدام الحواسيب – Computer Fraud and Abuse Act) (CFAA، ويُعاقب عليه بالسجن لسنوات عديدة بحسب جسامة الضرر[١]. وتُظهر قضايا شهيرة مثل "قضية آرون شوارتز" التفسير الواسع لهذا النص، حيث شمل تحميل عدد كبير من المقالات الأكاديمية من قاعدة بيانات دون إذن، كجريمة دخول غير مصرح به[٢].

أما في القانون الأوروبي، فتُعدّ المادة ٢ من "اتفاقية بودابست للجرائم السيبرانية" (٢٠٠١) مرجعاً أساسياً، حيث تُجرّم الوصول غير المشروع إلى النظم أو قواعد البيانات حتى لو لم تكن مشفّرة، واعتبرتها جريمة جنائية في حد ذاتها[٣]. وتُلزم الدول المصادقة عليها بتحديث تشريعاتها الداخلية لملاحقة هذه الأفعال.

وفي المنطقة العربية، نص قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨ على أن الدخول غير المشروع إلى قواعد البيانات الحكومية أو الخاصة يُعاقب عليه بالسجن المشدد وغرامات مالية باهظة، وقد تصل العقوبة إلى المؤبد في حالة اختراق نظم أمن قومي أو معلومات حساسة[٤]. ومثله القانون الإماراتي رقم ٥ لسنة ٢٠١٢ بشأن مكافحة جرائم تقنية المعلومات، الذي يغلّظ العقوبات على من يخترق أنظمة إلكترونية بقصد الاطلاع أو السرقة أو التعطيل[٥].

---

1 U.S. Code, Computer Fraud and Abuse Act (18 U.S.C. § 1030), 1986.

2 Electronic Frontier Foundation, Aaron Swartz Case Overview, 2013.

3 Council of Europe, Convention on Cybercrime (Budapest Convention), 2001, Article 2.

. قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨، المادة ٤١٤

. دولة الإمارات، قانون مكافحة جرائم تقنية المعلومات رقم ٥ لسنة ٢٠١٢، المادة 53

إنّ خطورة الوصول غير المشروع لا تكمن فقط في كسر الحواجز التقنية، بل في ما يترتب عليه من استغلال للمعلومات أو بيعها أو استخدامها لأغراض ضارة، ما يُظهر الحاجة إلى تعزيز الجوانب الوقائية بجانب الزجرية، مثل نظم الإنذار، التشفير، والتدريب الأمني الداخلي.

الفرع الثاني: التعديل أو التلاعب أو بيع البيانات دون إذن

تمثل عملية تعديل أو التلاعب بمحتوى قواعد البيانات دون إذن من المالك الشرعي، صورة أخرى خطيرة من صور الانتهاك، حيث تؤدي إلى فقدان الثقة في مصداقية البيانات، وتعريض مصالح الأفراد أو المؤسسات لأضرار مادية ومعنوية جسيمة. هذا النوع من الانتهاك غالباً ما يتم ضمن عمليات الاختراق المتقدمة أو عبر استغلال صلاحيات داخلية.(Insider Attacks)

في إطار القانون الأوروبي، تنص المادة ٤ من اتفاقية بودابست على تجريم "تعديل البيانات" دون وجه حق، سواء تم التعديل بشكل مباشر أو غير مباشر، كما اعتُبر إدخال معلومات زائفة أو حذف المعلومات جريمة قائمة بذاتها حتى دون مساس بالنظام المعلوماتي نفسه[١].

كذلك، يعالج قانون العقوبات الفرنسي في المادة ٣٢٣-٣ مسألة "إتلاف أو تعديل أو حذف بيانات رقمية"، ويُعاقب عليها بالسجن والغرامة، خاصة إذا تم الفعل عبر شبكة إلكترونية[٢]. بينما في الولايات المتحدة، يكمّل قانون CFAA الإطار القانوني، من خلال فرض عقوبات على كل من "يُلحق ضرراً متعمداً بالمعلومات المحمية"، ولو تم ذلك عبر تعديل طفيف[٣].

أما البيع غير المشروع للبيانات، فيُعدّ أحد أخطر أشكال الاستغلال غير المشروع، خاصة في ظل الأسواق السوداء الرقمية (Dark Web) التي تسوّق بيانات ملايين المستخدمين. وقد تصدت له معظم القوانين باعتباره جريمة مزدوجة: انتهاك للخصوصية واعتداء على الملكية الفكرية. ففي التشريع الأوروبي، تُعتبر إعادة استخدام قاعدة بيانات أو جزء منها لأغراض تجارية دون ترخيص انتهاكاً مباشراً للتوجيه ٩٦/٩/EC[4].

وفي السياق العربي، فإن قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠ يجرّم صراحة بيع أو مشاركة أو تداول بيانات شخصية بدون موافقة صريحة من صاحب البيانات، ويوقع غرامات

1 Council of Europe, Budapest Convention, Article 4.

2 Code Pénal Français, Article 323-3.

3 U.S. Department of Justice, CFAA Prosecution Guide, 2020.

4 Directive 96/9/EC of the European Parliament and of the Council, Article 7.

تصل إلى خمسة ملايين جنيه مصري[١]. ويُبرز هذا المسار أهمية مبدأ "الموافقة المسبقة" كمفتاح مشروع لأي معالجة أو تصرف.

وبذلك، فإن انتهاك الحق عبر التعديل أو البيع غير المشروع لا يُعدّ فقط إخلالاً بالحقوق القانونية للمالك، بل يهدد المنظومة الأخلاقية للتداول الرقمي، ويستدعي تعاوناً دولياً حقيقياً في إنفاذ القوانين.

المطلب الثاني: الآليات القانونية لحماية قواعد البيانات

الفرع الأول: الإجراءات القضائية والجزاءات المدنية والجنائية

تشكّل الإجراءات القضائية والجزاءات القانونية أداة حيوية لحماية قواعد البيانات الضخمة من الانتهاكات المختلفة، إذ توفر سبل إنفاذ الحقوق وتعويض المتضررين وردع المخالفين. تنص معظم التشريعات الوطنية والدولية على عقوبات متعددة تشمل التعويضات المالية، الحجز، وحتى العقوبات الجنائية.

تُعدّ الحماية السيبرانية الركيزة الأساسية لضمان سلامة قواعد البيانات الضخمة، بالنظر إلى تزايد حجم الهجمات الإلكترونية وتطور أساليب الاختراق. ويقتضي ذلك تبنّي منظومات أمنية متكاملة تشمل إجراءات المنع والكشف والاستجابة. فالاعتماد على تقنيات التشفير المتقدّمة، وأنظمة كشف التسلل (IDS/IPS)، وآليات إدارة المخاطر، أصبح من المتطلبات الجوهرية التي لا يمكن الاستغناء عنها لحماية البيانات ذات الطبيعة الحساسة أو العالية القيمة.

كما تؤكد المعايير الدولية، مثل ISO/IEC 27001 وNIST Cybersecurity Framework، على أهمية بناء بيئة أمنية قائمة على التقييم المستمر للثغرات، وتحديث بروتوكولات السلامة، وتطبيق قواعد التحكم في الوصول ، لضمان ألا يتمكن المستخدمون غير المصرح لهم من الوصول إلى البيانات أو تعديلها أو نسخها.

وتبرز كذلك أهمية التدريب المستمر للعاملين، واعتماد خطط استجابة للحوادث، وتوثيقها ومراجعتها دورياً، بما يعزز من جاهزية المؤسسات لمواجهة الهجمات المحتملة وتقليل آثارها. ويمثل دمج الأمن السيبراني ضمن دورة حياة إدارة البيانات شرطاً أساسياً لتحقيق حماية فعّالة ومستدامة.

في القانون الأوروبي، تُجرم التوجيهات والقوانين الوطنية الانتهاكات المتعلقة بقواعد البيانات عبر فرض غرامات مالية قد تصل إلى ملايين اليوروهات، إضافة إلى العقوبات الجنائية التي تشمل السجن في

---

١ قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠، المواد ١٨–٢١.

حالات التعدي الجسيم على حقوق المالك أو الاستخدام التجاري غير المشروع[١]. على سبيل المثال، يسمح النظام القانوني الألماني بمقاضاة المخالفين استناداً إلى قانون حماية قواعد البيانات، مع إمكانية طلب إيقاف الانتهاك وتعويض الأضرار المادية والمعنوية[٢].

أما في الولايات المتحدة، فيُعتمد نظام حقوق المؤلف مع القانون الخاص بجرائم الحاسوب(CFAA) ، حيث يمكن للمتضرر رفع دعاوى مدنية لاسترداد الأضرار الناجمة عن الاستنساخ أو الاستخدام غير المصرح به، كما تتوفر إجراءات جنائية لمحاكمة المتسللين والفاعلين.[٣] تُظهر قضايا قضائية عديدة مثل قضية Oracle ضد Google مدى جدية حماية قواعد البيانات عبر المحاكم المدنية والتقنية.

في الدول العربية، يوفر قانون مكافحة جرائم تقنية المعلومات في مصر والإمارات آليات قانونية فعالة تشمل الغرامات، السجن، وحتى الحجز على الأجهزة المستخدمة في ارتكاب الجريمة[٤]. كما يُمكن للمتضررين رفع دعاوى مدنية لإثبات الضرر والحصول على تعويضات، مما يعزز الحماية القضائية لقواعد البيانات.

وتُعتبر هذه الإجراءات القضائية ضرورية لإرساء سيادة القانون وحماية الحقوق الرقمية، لكنها غالباً ما تواجه تحديات في التطبيق العملي، مثل صعوبة إثبات الضرر، تعقيدات تحديد الجهة المعتدية، وصعوبة الملاحقة عبر الحدود.

تطبيقات قضائية عربية في حماية قواعد البيانات الضخمة

تظهر التطبيقات القضائية العربية أنّ مسألة حماية قواعد البيانات الرقمية ما تزال في مرحلة التشكل، إلا أنّ عدداً من الأحكام أرسى مبادئ مهمة يمكن الاستناد إليها في تأصيل الحماية القانونية لقواعد البيانات الضخمة. فقد قضت محكمة التمييز الأردنية في حكمها رقم (٣٩٢١/٢٠١٨) بأن قاعدة البيانات التي تتضمن "جهداً منهجياً في جمع المعلومات وترتيبها بما يحقق قيمة اقتصادية للمشروع" تُعد مالاً ذا قيمة قانونية يستوجب حماية من الاعتداء. وقد استندت المحكمة في ذلك إلى أن تجميع البيانات في حد ذاته يمثل استثماراً مالياً وفنياً يقتضي حماية مستقلة ولو لم يتوافر عنصر الابتكار الأدبي أو الفني.

1 Directive 2001/29/EC of the European Parliament on copyright, and related rights, Articles 7-8.

2 Bundesdatenschutzgesetz (BDSG), Germany, Sections 43-44.

3 U.S. Copyright Act, 17 U.S.C. §§ 501-505; Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030.

. قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨؛ قانون الإمارات رقم ٥ لسنة ٤٢٠١٢

كما أكدت محكمة القاهرة الاقتصادية في الدعوى رقم (١٠٢ لسنة ٢٠١٩ اقتصادي) أنّ الاستيلاء على قاعدة بيانات تخص شركة تجارية واستخدامها دون إذن "يشكل اعتداءً على حق استئثاري ناشئ عن جهد استثماري"، معتبرة أن الضرر لا يُقاس فقط بقيمة البيانات المسروقة بل بالأثر التجاري الناتج عن فقدان ميزة تنافسية. وقد ساهم هذا الحكم في تكريس مفهوم "القيمة الاقتصادية للبيانات" كأساس للتعويض.

أما محكمة دبي الابتدائية فقد تناولت في الحكم رقم (٢٠٢٠/٤٥ تجاري) واقعة تتعلق بسحب نسخ كبيرة من قاعدة بيانات عملاء إحدى الشركات عبر وسائل غير مشروعة، ورأت المحكمة أنّ "اختراق أنظمة الحماية بقصد الحصول على بيانات منظمة يشكل فعلاً غير مشروع مستقلّاً" حتى لو كانت البيانات في أصلها متاحة جزئياً للعامة. وهذا الاتجاه القضائي يعزّز فكرة أنّ معيار الحماية ليس نوع البيانات وإنما الجهد المبذول في تنظيمها ومعالجتها.

وتكشف هذه الأحكام مجتمعة أنّ القضاء العربي يميل تدريجياً إلى الاعتراف بقواعد البيانات الضخمة بوصفها أصولاً ذات قيمة اقتصادية تستحق حماية قانونية خاصة، اعتماداً على معيار الاستثمار والتنظيم وليس شرط الابتكار، وهو ما ينسجم مع الاتجاه التشريعي الدولي المعاصر.

الفرع الثاني: آليات الحماية التكنولوجية والرقمية (مثل التشفير والتتبع(...

بالإضافة إلى الحماية القانونية، تعتمد قواعد البيانات الضخمة على آليات تكنولوجية متقدمة تضمن سلامة البيانات وحمايتها من الانتهاك أو التلاعب. التشفير هو من أبرز هذه الآليات، حيث يتم تحويل البيانات إلى صيغة مشفرة لا يمكن قراءتها إلا بوجود مفتاح فك التشفير، مما يحد من خطر الوصول غير المصرح به أو التسرب[١].

تلعب تقنيات التتبع (Tracking) دوراً مهماً في مراقبة استخدام قواعد البيانات، إذ تسمح بتسجيل كل عملية وصول أو تعديل، وتحديد المصدر في حال وقوع خرق أمني. ومن أمثلة ذلك نظم الـ Blockchainالتي تستخدم في بعض قواعد البيانات لضمان الشفافية وعدم إمكانية التلاعب[٢].

كما تستخدم حلول إدارة الحقوق الرقمية (DRM) لضبط الوصول والنسخ، حيث تحدد الأذونات بدقة، وتمنع الاستنساخ أو التوزيع غير المرخص[٣]. وقد طورت شركات كبرى بروتوكولات أمان متكاملة تشمل

1 Stallings, William. Cryptography and Network Security: Principles and Practice, 7th Edition, 2017.

2 Crosby, Michael et al. "Blockchain Technology: Beyond Bitcoin." Applied Innovation Review, 2016.

3 DRM Consortium, Digital Rights Management Overview, 2020.

جدران الحماية(Firewalls) ، وأنظمة كشف التسلل(Intrusion Detection Systems) ، وتحديثات أمنية دورية لضمان الحد من الهجمات الإلكترونية.

ومن الضروري أن تكون الآليات التكنولوجية متكاملة مع الإطار القانوني، بحيث تضمن فعالية التنفيذ، وتسهّل إثبات الانتهاك أمام القضاء، كما تساعد في تحقيق الردع الوقائي. فعدم وجود حماية تقنية قوية يجعل القوانين دون جدوى في مواجهة الجرائم السيبرانية المعقدة.

فقرة تحليلية مقترحة:

تُظهر حالات الانتهاك المتزايدة لقواعد البيانات أنّ الآليات القانونية المعمول بها لم تعد كافية للحدّ من الاعتداءات الرقمية، إذ تتسم هذه الانتهاكات بالسرعة والتعقيد وصعوبة تتبّع مرتكبيها. كما أنّ الجزاءات المدنية والجنائية الحالية لا تواكب حجم الضرر الناتج عن تسريب البيانات أو الاستيلاء عليها، خصوصاً عندما يتعلق الأمر ببيانات حسّاسة أو ذات قيمة اقتصادية عالية. ويقود ذلك إلى ضرورة إعادة تقييم فعالية هذه الآليات، ودراسة إمكانية تبنّي نماذج تشريعية أكثر صرامة في مجال الأمن السيبراني وحماية البيانات.

أولًا: النتائج

١. تُظهر الدراسة أن قواعد البيانات الضخمة تمثل ركيزة أساسية في الاقتصاد الرقمي، وتسهم بشكل مباشر في دعم البحث العلمي وتطوير الخدمات الإلكترونية .
٢. يتبين وجود قصور في الأطر القانونية التقليدية في توفير حماية كافية وملائمة لقواعد البيانات الضخمة، خاصة في ظل التطورات التكنولوجية المتسارعة .
٣. تؤكد الدراسة أن الحماية القانونية المتخصصة تسهم في صون الحقوق الفكرية لأصحاب قواعد البيانات، وتعزز الثقة في الاستثمار الرقمي .
٤. تبرز الحاجة إلى تحقيق توازن تشريعي دقيق بين حماية حقوق الملكية الفكرية من جهة، وضمان حرية الوصول إلى البيانات وتشجيع الابتكار من جهة أخرى .
٥. يؤدي الإفراط في الحماية القانونية إلى آثار سلبية محتملة، من بينها تقييد البحث العلمي وإبطاء تطوير التقنيات الحديثة .
٦. تزداد التحديات القانونية تعقيدًا مع بروز تقنيات الذكاء الاصطناعي وتحليل البيانات الضخمة، مما يستدعي أطرًا قانونية أكثر مرونة وتخصصًا .
٧. تمثل الانتهاكات العابرة للحدود في مجال قواعد البيانات أحد أبرز التحديات التي تتطلب استجابة قانونية دولية منسقة .

ثانيًا: التوصيات

١. ضرورة استحداث إطار قانوني خاص ومتكامل لحماية قواعد البيانات الضخمة، يراعي خصوصيتها التقنية والاقتصادية .
٢. العمل على تحديث التشريعات الوطنية بما يتلاءم مع التحولات الرقمية المتسارعة، وبما يشمل تنظيم استخدام تقنيات الذكاء الاصطناعي في معالجة البيانات .
٣. تبني نهج تشريعي متوازن يضمن حماية الحقوق الفكرية دون الإخلال بمبادئ الابتكار وإتاحة الوصول المشروع إلى البيانات .
٤. النص صراحة على استثناءات قانونية واضحة لصالح البحث العلمي والاستخدامات التعليمية، بما يمنع تعطيل التقدم العلمي .
٥. تعزيز الآليات القانونية الخاصة بإنفاذ الحقوق، من خلال وضع جزاءات رادعة وإجراءات تنفيذ فعّالة لمواجهة الاعتداءات على قواعد البيانات .
٦. تطوير الأطر التنظيمية المتعلقة بترخيص استخدام البيانات، بما يضمن وضوح الحقوق والالتزامات بين الأطراف المختلفة .
٧. دعم بناء القدرات المؤسسية والقضائية في مجال حماية البيانات، من خلال التدريب المتخصص وتطوير الخبرات الفنية والقانونية .
٨. تعزيز التعاون الدولي عبر إبرام اتفاقيات ثنائية ومتعددة الأطراف، وتبادل المعلومات والخبرات لمواجهة الانتهاكات العابرة للحدود .
٩. العمل على توحيد أو تقارب المعايير القانونية الدولية المتعلقة بحماية قواعد البيانات، بما يحقق الاتساق في البيئة الرقمية العالمية.

المصادر والمراجع

١. دولة الإمارات، قانون مكافحة جرائم تقنية المعلومات رقم ٥ لسنة ٢٠١٢، المادة ٣.

٢. قانون حماية البيانات الشخصية المصري رقم ١٥١ لسنة ٢٠٢٠، المواد ١٨–٢١.

٣. قانون مكافحة الجرائم المعلوماتية بالإمارات (٢٠١٢)، المادة ٢٥، ص ٤٤–٤٦.

٤. قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨، المادة ١٤.

٥. قانون مكافحة جرائم تقنية المعلومات المصري رقم ١٧٥ لسنة ٢٠١٨؛ قانون الإمارات رقم ٥ لسنة ٢٠١٢.

٦. مفهوم قواعد البيانات الضخمة مستمد من NJS Shaba، Big Data Database، ص ١٧، ٣٥.

٧. وزارة الثقافة السعودية، اللائحة التنفيذية لحماية حقوق المؤلف والحقوق المجاورة، ٢٠٢١، المادة ١٨.

8. Amnesty International & Access Now, Surveillance Giants Report, 2020 .

9. Bundesdatenschutzgesetz (BDSG), Germany, Sections 43–44.

10. California Consumer Privacy Act (CCPA), Civil Code §§ 1798.100 et seq., California, 2020 .

11. Code de la propriété intellectuelle, Article L341-1, France, 2021 .

12. Code Pénal Français, Article 323-3.

13. Copyright Act (USA).١٠٦ ، القسم

14. Council of Europe, Budapest Convention, Article 4.

15. Council of Europe, Convention on Cybercrime (Budapest Convention), 2001, Article 2.

16. CQUSA ،Computer Fraud and Abuse Act, § 1030.٢٠٢١ ، تحديثات

17. Crosby, Michael et al. "Blockchain Technology: Beyond Bitcoin." Applied Innovation Review, 2016.

18. Database Directive 96/9/EC“ الموسوعة القانونية البريطانية، ”Database right ؛ ص

19. Directive 2001/29/EC of the European Parliament on copyright, and related rights, Articles 7–8.

20. Directive 96/9/EC of the European Parliament and of the Council, Article 7.
21. DRM Consortium, Digital Rights Management Overview, 2020.
22. Electronic Frontier Foundation, Aaron Swartz Case Overview, 2013.
23. European Commission ،Directive (EU) 2019/1024 on open data and the re-use of public sector information, 2019 ؛European data strategy ، .٢٠٢٠
24. European Parliament, Directive 96/9/EC on the legal protection of databases, 1996 .
25. European Union, General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, Article 32 .
26. Feist Publications, Inc. v. Rural Telephone Service Co., 1991
27. Hamza & Pradana ،"A Survey of Intellectual Property Rights بداية ،"... المقال استرفاق مفاهيم الحقوق، Algorithms 15(11).٢٠٢٢ ،
28. Ibid., Article 33 .
29. Jane Doe ،"Database Protection in the USA: The Limitations of Copyright Law" ،JIPLR.١٣–١٢ ص ،٢٠٢٠ ،
30. Jennifer Granick ،Spot a Bug, Go to Jail ،Wired 2006.
31. Knowledge commons ،Wikipedia.
32. Law Commission (UK) ،Database Right after Brexit, 2021.٩–٨ ص ،
33. McCarthy Tétrault LLP ،Big Data Legal Aspects (Canada) ،Feb 22 2016.٤–٣ ص ،
34. Ministère de la Culture (France) ،Code de la propriété intellectuelle, 2022.٢٧٦–٢٧٤ ص ،
35. P Andanda ،"Towards a Paradigm Shift in Governing Data Access and ...".٢٠١٩ ،
36. Pamela Samuelson, "Possible Futures of Fair Use," University of Colorado Law Review, vol. 90, 2019, pp. 727–780 .

37. R Hamza & H Pradana ،"A Survey of Intellectual Property Rights Protection in Big Data Applications" ،Algorithms 15(11).٢٠٢٢ ،
38. Sardor Shukhratovich Mamanazarov ،"Intellectual Property Theories as Applied to Big Data".٦–٥ ص ،٢٠٢٣ ،
39. Stallings, William. Cryptography and Network Security: Principles and Practice, 7th Edition, 2017.
40. The European Parliament Council ،Directive 96/9/EC on the legal protection of databases, 1996.
41. The European Parliament Council ،Directive 96/9/EC on the legal protection of databases.
42. U.S. Code, Computer Fraud and Abuse Act (18 U.S.C. § 1030), 1986.
43. U.S. Copyright Act, 17 U.S.C. § 1201, DMCA .
44. U.S. Copyright Act, 17 U.S.C. §§ 501–505; Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030.
45. U.S. Department of Justice, CFAA Prosecution Guide, 2020.
46. UK Parliament ،Computer Misuse Act 1990.
47. Wikipedia ،Database right ؛Database Directive 96/9/EC.
48. Wikipedia ،General Data Protection Regulation آمن المعلومات والبيانات , الشخصية.

WTO ،TRIPS Agreement, 1994١٠ المادة ،١ الجزء ،