International Journal for Scientific Research (IJSR)
المجلة الدولية للبحوث العلمية
Vol. (4), No. (10) October 2025 الإصدار (4)، العدد (10)

حماية البيانات الشخصية للشركات والمؤسسات والأفراد وفقاً للمعايير الدولية وأحكام القانون الدولي الخاص

تمام عبداللطيف الجيجكلي
بكالوريوس كلية الحقوق، جامعة حلب، سوريا
tammam.s@brightwires.com.sa

مستخلص البحث

يهدف هذا البحث إلى دراسة الإطار القانوني والتنظيمي لحماية البيانات الشخصية في سياق الاستخدام المتزايد لها من قبل الشركات، المؤسسات، والأفراد، خاصة في ظل الطفرة التكنولوجية والتحول الرقمي العالمي. وتتمحور الدراسة حول تحليل المعايير الدولية البارزة، وعلى رأسها اللائحة العامة لحماية البيانات (GDPR) الصادرة عن الاتحاد الأوروبي، بالإضافة إلى المبادئ التوجيهية الصادرة عن منظمات دولية كمنظمة التعاون الاقتصادي والتنمية (OECD). كما يتناول البحث الجوانب المتعلقة بالقانون الدولي الخاص، لا سيما التحديات القانونية المترتبة على نقل البيانات عبر الحدود الوطنية، وتضارب التشريعات بين الدول، مما يطرح إشكاليات قانونية معقدة تتطلب تنسيقًا دوليًا فعالًا. ويستعرض البحث كذلك مسؤوليات الشركات والمؤسسات في تبني سياسات حماية خصوصية صارمة، وضمان أمن البيانات التي تجمعها وتعالجها، إلى جانب دور الأفراد في حماية بياناتهم الشخصية. خلصت الدراسة إلى أن حماية البيانات الشخصية لم تعد مسألة داخلية بحتة، بل أصبحت قضية عالمية تتطلب تكاملًا بين القوانين الوطنية والمعايير الدولية، وتعاونًا دوليًا لضمان حماية فعالة وشاملة، في ظل بيئة رقمية عابرة للحدود ومتغيرة باستمرار.

الكلمات المفتاحية: حماية البيانات الشخصية، الخصوصية الرقمية، الشركات والمؤسسات، الأفراد، الأمن السيبراني.

International Journal for Scientific Research (IJSR)

المجلة الدولية للبحوث العلمية

Vol. (4), No. (10) October 2025 الإصدار (4)، العدد (10)

Protecting the personal data of companies, institutions, and individuals in accordance with international standards and the provisions of private international law.

Tammam Abdul Latif Al-Jijakli
Bachelor of Law, University of Aleppo, Syria
tammam.s@brightwires.com.sa

Abstract

This research aims to examine the legal and regulatory framework for protecting personal data in the context of its increasing use by companies, institutions, and individuals, especially in light of the technological boom and global digital transformation. The study focuses on analyzing prominent international standards, most notably the General Data Protection Regulation (GDPR) issued by the European Union, in addition to the research also addresses aspects related to private international law, particularly the legal challenges arising from the transfer of data across national borders and the conflicting laws between countries, which pose complex legal issues that require effective international coordination. The research also examines the responsibilities of companies and organizations in adopting strict privacy protection policies and ensuring the security of the data they collect and process, as well as the role of individuals in protecting their personal data. The study concluded that personal data protection is no longer a purely domestic issue, but rather a global one that requires integration between national laws and international standards, as well as international cooperation to ensure effective and comprehensive protection in a constantly changing, cross-border digital environment.

Keywords: Personal Data Protection, Digital Privacy, Companies and Institutions, Individuals, Cybersecurity.

المقدمة

في ظل التطور المتسارع للتكنولوجيا الرقمية وانتشار استخدام الإنترنت والذكاء الاصطناعي، أصبحت البيانات الشخصية موردًا بالغ الأهمية في مختلف مجالات الحياة، سواء على صعيد الأفراد أو الشركات والمؤسسات. ومع تزايد الاعتماد على هذه البيانات في تقديم الخدمات، وتحليل السلوك، واتخاذ

القرارات التجارية، برزت الحاجة الملحة إلى تنظيم جمعها واستخدامها وتخزينها بما يحفظ خصوصية الأفراد ويحمي المصالح الاقتصادية والتجارية للمؤسسات[1].

لقد باتت حماية البيانات الشخصية من أبرز التحديات القانونية في العصر الرقمي، حيث تنطوي عمليات المعالجة على مخاطر جسيمة، تشمل الاختراقات الأمنية، وسوء الاستخدام، والإتجار غير المشروع بالمعلومات. وانطلاقًا من هذه المخاطر، عملت العديد من الأنظمة القانونية الوطنية والدولية على سنّ تشريعات ومعايير تهدف إلى ضمان الاستخدام المشروع والمسؤول للبيانات الشخصية، مع توفير سبل الانتصاف القانونية في حال وقوع انتهاكات.

تسعى هذه الدراسة إلى تسليط الضوء على الأطر القانونية والتنظيمية التي تحكم حماية البيانات الشخصية، مركّزة على المعايير الدولية البارزة مثل اللائحة العامة لحماية البيانات في الاتحاد الأوروبي (GDPR)، إضافة إلى استعراض أحكام القانون الدولي الخاص التي تعالج الإشكاليات الناتجة عن نقل البيانات عبر الحدود، وتنازع القوانين الوطنية في هذا المجال. كما يتناول البحث مسؤوليات الشركات والمؤسسات في تبني سياسات فعالة لحماية البيانات، ودور الأفراد في حماية خصوصيتهم في بيئة رقمية متغيرة ومعقدة.

ومن خلال هذه الدراسة، سيتم تحليل أبرز التحديات التي تواجه تطبيق هذه المعايير، واقتراح حلول عملية لتعزيز حماية البيانات في إطار قانوني دولي متماسك وعادل.

أهمية الموضوع

تنبع أهمية هذا الموضوع من الواقع الرقمي المعاصر الذي أصبحت فيه البيانات الشخصية عنصرًا أساسيًا في مختلف التعاملات اليومية، سواء على مستوى الأفراد أو الشركات والمؤسسات. فمع التوسع في استخدام التكنولوجيا، وتزايد الاعتماد على الإنترنت والخدمات السحابية، باتت كميات هائلة من البيانات تُجمع وتُعالج وتُنقل عبر الحدود، ما يثير تحديات قانونية وأمنية كبيرة.

ولأن انتهاك الخصوصية أو إساءة استخدام البيانات قد يؤدي إلى أضرار جسيمة تمس الحقوق الأساسية للأفراد، وتؤثر على الثقة في البيئة الرقمية، فإن وضع إطار قانوني فعال لحمايتها يُعد ضرورة ملحّة. كما أن المؤسسات والشركات أصبحت مطالبة بالامتثال لمعايير دولية صارمة، مثل اللائحة العامة لحماية البيانات (GDPR)، التي لا تقتصر آثارها على الدول الأوروبية فقط، بل تمتد عالميًا لتشمل كل جهة تتعامل مع بيانات مواطني الاتحاد الأوروبي.

[1] أشرف جابر سيد، الجوانب القانونية لمواقع التواصل الاجتماعي، دار النهضة العربية، القاهرة، 2013.

ويزداد الموضوع أهمية في إطار القانون الدولي الخاص، نظرًا لتعدد الأطراف المعنية، وتضارب القوانين الوطنية، وصعوبة إنفاذ الأحكام في القضايا العابرة للحدود. لذا فإن فهم هذه المنظومة القانونية المتشابكة يُسهم في تعزيز حماية البيانات، ويدعم الاستقرار القانوني والاقتصادي في عالم رقمي لا يعترف بالحدود[2].

مشكلة البحث

تتمثل مشكلة هذا البحث في التحدي المتزايد الذي يواجهه الأفراد والشركات والمؤسسات في سبيل حماية بياناتهم الشخصية في ظل التطور التكنولوجي المتسارع، وتوسع استخدام البيانات في مختلف المجالات. إذ يُطرح التساؤل حول مدى كفاية وفعالية الأطر القانونية الحالية، سواء على المستوى الدولي أو في إطار القانون الدولي الخاص، في تنظيم جمع البيانات الشخصية ومعالجتها ونقلها، خاصة في ظل التباين بين التشريعات الوطنية وصعوبة إنفاذ القوانين عبر الحدود.

ويزداد تعقيد المشكلة مع تعدد الجهات التي تتعامل مع البيانات، وغياب معايير موحدة عالميًا، ما يؤدي إلى تهديدات جدية لخصوصية الأفراد، ومخاطر قانونية وتجارية على الشركات والمؤسسات. كما أن ضعف التنسيق الدولي يطرح تحديات كبيرة أمام حماية هذه البيانات في البيئة الرقمية العالمية.

بالتالي، يسعى البحث إلى معالجة التساؤل الرئيسي الآتي:

إلى أي مدى تساهم المعايير الدولية وأحكام القانون الدولي الخاص في توفير حماية فعالة للبيانات الشخصية للأفراد والشركات والمؤسسات، في ظل التحديات القانونية والتقنية العابرة للحدود؟

أهدف البحث

يهدف البحث إلى:

1. توضيح المفهوم القانوني للبيانات الشخصية، وتحديد نطاقها وحدودها في السياق الرقمي الحديث، سواء بالنسبة للأفراد أو الشركات والمؤسسات.
2. تحليل الإطار القانوني الدولي لحماية البيانات الشخصية، خاصة المعايير الدولية المعتمدة مثل اللائحة العامة لحماية البيانات (GDPR)، ومبادئ منظمة التعاون الاقتصادي والتنمية (OECD).
3. دراسة أحكام القانون الدولي الخاص المتعلقة بحماية البيانات، ولا سيما ما يتعلق بتنازع القوانين،

[2] باسل فايز حمد القطاطشة، ممدوح حسن العدوان، الحماية الجنائية لخصوصية البيانات الشخصية الرقمية، دراسة مقارنة، رسالة دكتوراه، جامعة العلوم الإسلامية، عمان، 2022.

والاختصاص القضائي، ونقل البيانات عبر الحدود.

4. رصد التحديات القانونية والفنية التي تواجه حماية البيانات في البيئة الرقمية، سواء على المستوى الوطني أو الدولي.
5. تقييم مدى التزام الشركات والمؤسسات بالمعايير الدولية في حماية البيانات، وتحليل مسؤولياتها القانونية والأخلاقية في هذا المجال.
6. تقديم مقترحات وتوصيات قانونية لتعزيز فعالية حماية البيانات الشخصية، وتحقيق التوازن بين الابتكار التكنولوجي ومتطلبات الخصوصية.

منهج الدراسة

يعتمد هذا البحث على المنهج الوصفي التحليلي باعتباره الأنسب لدراسة وتحليل القواعد القانونية المتعلقة بحماية البيانات الشخصية، سواء على المستوى الدولي أو ضمن أحكام القانون الدولي الخاص. ويتضمن ذلك وصف الأطر التشريعية والتنظيمية القائمة، وتحليل نصوصها القانونية وأحكامها، مع استعراض التطبيقات العملية المرتبطة بها.

كما يستعين البحث بالمنهج المقارن في تحليل النماذج القانونية المختلفة لحماية البيانات، مثل المقارنة بين اللائحة العامة لحماية البيانات الأوروبية (GDPR) وبعض التشريعات الوطنية في دول أخرى، بهدف الوقوف على أوجه التشابه والاختلاف ومدى التوافق مع المعايير الدولية.

ويتم أيضًا توظيف المنهج الاستقرائي من خلال تتبّع التطورات القانونية والتقنية المرتبطة بحماية البيانات الشخصية، لا سيما تلك المتعلقة بنقل البيانات عبر الحدود والاختصاص القضائي، وذلك لفهم التحديات المعاصرة واستخلاص النتائج.

أخيرًا، يعتمد البحث على تحليل السوابق القضائية والاتفاقيات الدولية ذات الصلة، وكذلك التقارير الصادرة عن الهيئات الدولية ومنظمات حماية الخصوصية، بهدف دعم الدراسة بأمثلة عملية ومعايير معتمدة دوليًا.

خطة البحث

- المقدمة.
- أهمية الموضوع.
- تحديد إشكالية البحث.

- أهداف البحث.
- منهجية البحث.
- خطة البحث:

وقد قام الباحث بتقسيم البحث إلى ثمانية مباحث كالآتي:

- **المبحث الأول:** مفهوم البيانات الشخصية وأنواعها
- **المبحث الثاني:** التطور التاريخي والتشريعي لحماية البيانات
- **المبحث الثالث:** اللائحة العامة لحماية البيانات الأوروبية (GDPR)
- **المبحث الرابع:** المبادئ الدولية الأخرى لحماية البيانات
- **المبحث الخامس:** تنازع القوانين والاختصاص القضائي في قضايا البيانات
- **المبحث السادس:** الحلول القانونية لحماية البيانات عبر الحدود
- **المبحث السابع:** التزامات الشركات تجاه الأفراد
- **المبحث الثامن:** المسؤولية القانونية والعقوبات المترتبة على الإخلال

- الخاتمة.
- النتائج المستخلصة.
- التوصيات.
- المصادر والمراجع.

المبحث الأول: مفهوم البيانات الشخصية وأنواعها

أولًا: مفهوم البيانات الشخصية:

تشير البيانات الشخصية إلى أي معلومات تتعلق بشخص طبيعي يمكن التعرف عليه بشكل مباشر أو غير مباشر، من خلال هذه المعلومات أو من خلال الربط بينها وبين بيانات أخرى[3].

وقد عرفتها اللائحة العامة لحماية البيانات الأوروبية (GDPR) في المادة (4) بأنها:

"أي معلومات تتعلق بشخص طبيعي محدد أو قابل للتحديد؛ ويُعدّ الشخص قابلاً للتحديد إذا كان بالإمكان التعرف عليه بشكل مباشر أو غير مباشر، وخاصة بالرجوع إلى معرف مثل الاسم أو رقم الهوية أو بيانات الموقع أو معرف عبر الإنترنت أو إلى عنصر واحد أو أكثر من الخصائص الخاصة بهوية ذلك

[3] بوكر رشيدة، تحديات العصر في مواجهة خطط حماية الحق في الخصوصية، مجلة حقوق الإنسان والحريات العامة، مج7، ع2، 2022.

الشخص البدنية أو الفسيولوجية أو الجينية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية." ويُشترط في البيانات الشخصية أن: تتعلق بشخص طبيعي (أي لا تنطبق على الأشخاص الاعتباريين كالشركات)، وتكون كافية لتحديد هويته أو المساعدة في ذلك.

ثانيًا: أنواع البيانات الشخصية:

يمكن تصنيف البيانات الشخصية إلى عدة أنواع، وذلك بحسب درجة حساسيتها أو الغرض من استخدامها:

1. البيانات التعريفية (Identification Data): وتشمل المعلومات التي تُعرّف بالشخص بشكل مباشر. مثل: الاسم الكامل، رقم الهوية أو الجواز، تاريخ الميلاد، رقم الهاتف، العنوان البريدي، البريد الإلكتروني.
2. البيانات البيومترية (Biometric Data): بيانات تُستخرج من الخصائص الجسدية أو السلوكية الفريدة للشخص. مثل: بصمات الأصابع، بصمة العين أو الوجه، نبرة الصوت، أنماط المشي أو التوقيع اليدوي.
3. البيانات الصحية والطبية (Health Data): تتعلق بالحالة الصحية أو التاريخ الطبي للفرد. مثل: نتائج التحاليل، السجلات الطبية، الإعاقات أو الأمراض المزمنة، بيانات التأمين الصحي.
4. البيانات المالية والاقتصادية: مثل: الحسابات البنكية، تفاصيل البطاقة المصرفية، معلومات الدخل والضرائب، التاريخ الائتماني.
5. البيانات الرقمية والسلوكية: تُجمع من خلال تفاعل الشخص مع الإنترنت والتقنيات الحديثة. مثل: عنوان IP، سجل التصفح، سجل البحث، الموقع الجغرافي GPS، ملفات تعريف الارتباط (Cookies).
6. البيانات الحساسة (Sensitive Personal Data): وهي أكثر أنواع البيانات حساسية، وتحتاج لحماية قانونية خاصة. مثل: الأصل العرقي أو الإثني، الآراء السياسية، المعتقدات الدينية أو الفلسفية، الانتماء النقابي، الميول الجنسية.

في العديد من التشريعات، يُمنع جمع أو معالجة هذه البيانات إلا بشروط صارمة أو بموافقة صريحة من الشخص المعني.

الفرق بين حماية البيانات والخصوصية[4]:

حماية البيانات	الخصوصية
تعريف: مجموعة الإجراءات والتقنيات والسياسات التي تهدف إلى تأمين البيانات الشخصية من الوصول غير المصرح به، أو الفقدان، أو التعديل، أو التسريب.	تعريف: حق الفرد في التحكم بالمعلومات التي تخصه، والقدرة على تحديد من يمكنه الوصول إلى بياناته وكيفية استخدامها.
الهدف: ضمان سلامة البيانات وحمايتها من التهديدات الأمنية أو الاستخدام غير المشروع.	الهدف: حماية حرية الفرد وكرامته، ومنع التدخل غير المبرر في حياته الشخصية.
التركيز: على الجوانب التقنية والتنظيمية (مثل التشفير، إدارة الوصول، السياسات الأمنية).	التركيز: على الجوانب القانونية والأخلاقية المتعلقة بحقوق الأفراد في التحكم ببياناتهم.
المسؤولية: تقع على عاتق المؤسسات والشركات التي تجمع وتعالج البيانات لضمان أمانها.	المسؤولية: تقع على الأفراد والجهات معًا، حيث يحق للفرد حماية خصوصيته، وللمؤسسات احترام هذا الحق.
مثال: استخدام جدران حماية (Firewall)، تشفير البيانات، النسخ الاحتياطي، التحكم في الوصول.	مثال: حق الشخص في معرفة نوع البيانات التي تُجمع عنه، وطلب حذف بياناته، والموافقة أو الرفض على مشاركة بياناته.

المبحث الثاني: التطور التاريخي والتشريعي لحماية البيانات

1. البدايات المبكرة:

في النصف الثاني من القرن العشرين، مع انتشار الحواسيب والأنظمة الإلكترونية، بدأ القلق يزداد حول جمع وتخزين المعلومات الشخصية بشكل آلي.

أولى الخطوات جاءت مع صدور قوانين ومبادرات لحماية الخصوصية في الدول الغربية، مثل قانون حماية الخصوصية في السويد عام 1973، والذي يُعد من أوائل القوانين الوطنية التي تناولت حماية البيانات الشخصية.

2. ظهور القوانين الوطنية[5]:

خلال الثمانينات والتسعينات، تبنت عدة دول قوانين وطنية تهدف إلى تنظيم جمع واستخدام البيانات الشخصية.

مثال بارز: قانون حماية البيانات في المملكة المتحدة عام 1984، وقانون حماية البيانات الألماني.

هذه القوانين ركزت على مبادئ مثل جمع البيانات بشكل قانوني، وعدم الإفراط في جمع البيانات، وحق الأفراد في الاطلاع على بياناتهم وتصحيحها.

[4] رانيا سليمان ابو المعاطي محمود، ونهي محمد ابراهيم الدسوقي، وفاتن فايز حميدة الصفتي، سياسة مكافحة الإرهاب الإلكتروني، مصر والسعودية أنموذجاً، المركز العربي للبحوث والدراسات، آفاق سياسية، ع53، 2020.

[5] سليم محمد سليم حسين، الحماية الجنائية للبيانات الشخصية المعالجة آليا، دراسة مقارنة، مجلة العلوم القانونية والاقتصادية، كلية الحقوق جامعة عين شمس، مج62، ع1، 2020.

3. التنظيم الدولي:

مع تزايد التبادل التجاري والمعلوماتي عبر الحدود، ظهرت الحاجة إلى معايير دولية. منظمة التعاون الاقتصادي والتنمية (OECD) أصدرت في عام 1980 مبادئ حماية الخصوصية وحماية البيانات، التي تضمنت مبادئ مثل:

- الحد من جمع البيانات.
- جودة البيانات.
- الأمان.
- الشفافية.
- حقوق الوصول والتصحيح.

كذلك، أصدرت الأمم المتحدة توصيات لدعم حقوق الخصوصية وحماية البيانات.

4. اللائحة العامة لحماية البيانات: (GDPR)

في عام 2016، أصدر الاتحاد الأوروبي اللائحة العامة لحماية البيانات (GDPR) التي دخلت حيز التنفيذ في مايو 2018، والتي تمثل نقلة نوعية في حماية البيانات الشخصية على مستوى عالمي[6].

تميزت GDPR بفرضها قواعد صارمة على معالجة البيانات الشخصية، وتوسيع حقوق الأفراد، وتحديد مسؤوليات واضحة على عاتق المؤسسات.

أصبحت GDPR معيارًا دوليًا يُحتذى به، وأثرت على سياسات وحوكمة البيانات في العديد من دول العالم.

5. التحديات الحديثة والتشريعات الجديدة:

مع تطور التكنولوجيا الحديثة مثل الذكاء الاصطناعي، وإنترنت الأشياء، والتقنيات البيومترية، ظهرت تحديات جديدة تتطلب تحديث التشريعات.

دول عديدة تعمل على تطوير قوانين حماية البيانات لمواكبة هذه التطورات، مثل قانون حماية البيانات في كاليفورنيا (CCPA) في الولايات المتحدة، وقوانين حماية البيانات في دول عربية مثل الإمارات والسعودية.

[6] شلواح ميرة، بشيري كهينة، المسؤولية المدنية عن انتهاك حق الخصوصية في المجال الرقمي، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة عبدالرحمان ميرة، بجاية، 2019-2020.

خلاصة:

حماية البيانات الشخصية مرت بمراحل تطور متسارعة من قوانين وطنية محدودة إلى أطر تشريعية دولية شاملة. ويستمر التطور لمواجهة التحديات التقنية والقانونية الجديدة، مع التركيز على التوازن بين الابتكار وحماية الحقوق الفردية.

المبحث الثالث: اللائحة العامة لحماية البيانات الأوروبية (GDPR)

اللائحة العامة لحماية البيانات الأوروبية: (GDPR)

1. تمهيد:

اللائحة العامة لحماية البيانات (General Data Protection Regulation -GDPR) هي قانون أوروبي دخل حيز التنفيذ في **25 مايو 2018**، ويهدف إلى تنظيم معالجة البيانات الشخصية للأفراد داخل الاتحاد الأوروبي، وتعزيز حماية خصوصيتهم في العصر الرقمي[7].

2. أهداف اللائحة:

- حماية حقوق الأفراد في الخصوصية والسيطرة على بياناتهم الشخصية.
- توحيد قواعد حماية البيانات عبر دول الاتحاد الأوروبي.
- تعزيز الشفافية والمساءلة لدى المؤسسات والشركات التي تجمع وتعالج البيانات.
- ضمان حرية تدفق البيانات داخل السوق الأوروبية المشتركة مع الحفاظ على الحماية الكافية.

3. النطاق التطبيقي:

- تنطبق GDPR على جميع الشركات والمؤسسات التي تعالج بيانات شخصية للأفراد المقيمين في الاتحاد الأوروبي، سواء كانت هذه الشركات داخل الاتحاد أو خارجه.
- تشمل أيضًا المعالجة الإلكترونية واليدوية للبيانات الشخصية.

4. المبادئ الأساسية في: GDPR

- **الشرعية، الإنصاف والشفافية:** معالجة البيانات بشكل قانوني وعادل وبشفافية تامة.

[7] طارق جمعه السيد راشد، الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي، دراسة مقارنة، مجلة القانون والاقتصاد، كلية الحقوق، جامعة القاهرة، ملحق خاص، ع92، بدون سنة.

- **تحديد الغرض:** جمع البيانات لاستخدام محدد وواضح فقط.
- **تقليل البيانات:** جمع أقل كمية ممكنة من البيانات الضرورية فقط.
- **دقة البيانات:** التأكد من صحة البيانات وتحديثها.
- **تخزين محدود:** عدم الاحتفاظ بالبيانات لفترة أطول من اللازم.
- **السلامة والسرية:** حماية البيانات من الوصول أو الفقدان أو التسريب.
- **المسؤولية:** تحمل المؤسسات مسؤولية تطبيق هذه المبادئ وإثبات الالتزام بها.

5. حقوق الأفراد بموجب: GDPR

- **الحق في الوصول:** معرفة ما إذا كانت بياناتهم تُعالج والحصول على نسخة منها.
- **الحق في التصحيح:** طلب تعديل البيانات غير الدقيقة أو الناقصة.
- **الحق في المحو ("الحق في النسيان"):** طلب حذف بياناتهم في ظروف معينة.
- **الحق في تقييد المعالجة:** الحد من معالجة بياناتهم في حالات معينة.
- **الحق في نقل البيانات:** نقل بياناتهم إلى جهة أخرى.
- **الحق في الاعتراض:** الاعتراض على معالجة بياناتهم لأسباب تتعلق بوضعهم الخاص.
- **حقوق تتعلق بالقرارات الآلية:** حماية الأفراد من اتخاذ قرارات أو تحليلات تعتمد فقط على المعالجة الآلية.

6. التزامات الشركات والمؤسسات:

- تعيين مسؤول حماية البيانات (Data Protection Officer) في بعض الحالات.
- إجراء تقييمات تأثير على الخصوصية قبل معالجة البيانات.
- الإبلاغ عن أي خرق أمني للبيانات خلال 72 ساعة.
- تطبيق إجراءات تقنية وتنظيمية لضمان حماية البيانات.
- الاحتفاظ بسجلات معالجة البيانات.

7. العقوبات والغرامات:

- يمكن فرض غرامات مالية ضخمة تصل إلى 20 مليون يورو أو 4% من إجمالي إيرادات الشركة السنوية، أيهما أكبر، على المؤسسات التي تخالف اللائحة[8].

خلاصة:

GDPR تعتبر من أقوى القوانين لحماية البيانات الشخصية في العالم، وأثرت على صياغة سياسات حماية البيانات خارج أوروبا أيضًا، حيث أصبحت معيارًا دوليًا للخصوصية والأمان.

المبحث الرابع: المبادئ الدولية الأخرى لحماية البيانات

1. مبادئ منظمة التعاون الاقتصادي والتنمية (OECD) لحماية الخصوصية وحماية البيانات (1980):

- تعتبر هذه المبادئ من أول المبادئ الدولية التي وضعت إطارًا لحماية البيانات الشخصية، وركزت على توازن حماية الخصوصية مع حرية تدفق المعلومات.
- أهم المبادئ:

- **حدود جمع البيانات:** جمع البيانات يكون قانونيًا وبتصريح واضح.
- **جودة البيانات:** يجب أن تكون البيانات دقيقة وكاملة ومحدثة.
- **الغرض من جمع البيانات:** يجب تحديد غرض واضح لجمع البيانات.
- **القيود على استخدام البيانات:** استخدام البيانات يكون ضمن الأغراض المصرح بها فقط.
- **الأمان:** حماية البيانات من الوصول غير المصرح به أو الفقدان.
- **الشفافية:** يجب إعلام الأفراد بجمع واستخدام بياناتهم.
- **المشاركة أو الإفصاح:** لا يتم الإفصاح عن البيانات لأطراف أخرى إلا بشروط معينة.
- **المسؤولية:** وجود آليات للامتثال للمبادئ والرد على الشكاوى.

2. إعلان الأمم المتحدة لحقوق الإنسان (المادة 12):

- ينص على حق كل فرد في الخصوصية، وحماية حياته الخاصة والعائلية، وحقه في عدم التدخل

[8] طارق جمعه السيد راشد، الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي، دراسة مقارنة، مجلة القانون والاقتصاد، كلية الحقوق، جامعة القاهرة، ملحق خاص، ع92، بدون سنة.

أو الاعتداء على شرفه وسمعته[9].

3. الإطار الأوروبي للحماية (اتفاقية رقم 108 لمجلس أوروبا):

- أول اتفاقية دولية ملزمة لحماية الأشخاص فيما يتعلق بمعالجة البيانات الشخصية، صادقت عليها عدة دول أوروبية.
- تتضمن قواعد لحماية الخصوصية وحرية نقل البيانات بين الدول.

4. إعلان الخصوصية الأمريكي: (Fair Information Practice Principles -FIPPs)

- وضعت من قبل مكتب التجارة الأمريكية في السبعينيات، وتُستخدم كأساس في العديد من القوانين الأمريكية.
- تشمل مبادئ مثل: الإخطار، الاختيار، الوصول، الأمان، المسؤولية[10].

5. المبادئ الإقليمية:

- **في أمريكا اللاتينية:** إطار قانوني لحماية البيانات مثل قانون "LGPD" في البرازيل.
- **في آسيا:** دول مثل اليابان وكوريا الجنوبية لديها تشريعات متقدمة لحماية البيانات.
- **في الدول العربية:** مبادرات حديثة لتطوير قوانين تتماشى مع المعايير الدولية.

خلاصة:

تتسم المبادئ الدولية لحماية البيانات بالتركيز على حقوق الأفراد في الخصوصية، وضمان جمع واستخدام البيانات بشفافية وأمان، مع توفير آليات للمساءلة والامتثال. وتكمل هذه المبادئ بعضها، وتُعتبر المرجع الأساسي للدول في صياغة قوانينها الوطنية.

المبحث الخامس: تنازع القوانين والاختصاص القضائي في قضايا البيانات

1. مفهوم تنازع القوانين: (Conflict of Laws)

- هو الحالة التى تنشأ عندما يكون هناك أكثر من نظام قانوني دولي أو وطني يمكن أن ينطبق على قضية معينة، مما يثير سؤال: أي قانون يجب أن يُطبّق؟

[9] عزت عبدالمحسن ابراهيم، الحق في الخصوصية الرقمية وتحديات عصر التقنية، مجلة العلوم القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، مج62، ع1، 2020.

[10] علاء الدين عبدالله فواز الخصاونة، الحماية القانونية للخصوصية والبيانات الشخصية في نطاق المعلوماتية، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، جامعة الشارقة، مج8، ع2، 2011.

- في مجال حماية البيانات، تتعدد التشريعات الوطنية والدولية التي قد تختلف في شروط حماية البيانات، ما يخلق تعقيدات في تحديد القانون الواجب التطبيق[11].

2. مفهوم الاختصاص القضائي: (Jurisdiction)

- يشير إلى سلطة المحكمة أو الجهة القضائية للنظر في النزاع وصدور حكم فيه.
- في قضايا البيانات، يبرز السؤال: أي دولة أو محكمة لها الحق في الفصل في النزاع المتعلق بالبيانات؟

3. التحديات في قضايا البيانات الشخصية:

- **عبور البيانات للحدود:** البيانات تنتقل إلكترونيًا بين دول مختلفة، ما يجعل تحديد القانون والاختصاص معقدًا.
- **تعدد التشريعات:** اختلاف قواعد حماية البيانات بين الدول، مثل بين الاتحاد الأوروبي (GDPR) والولايات المتحدة، أو بين دول ذات قوانين ضعيفة وأخرى صارمة.
- **تحديد مقر المعالجة:** هل القانون الواجب التطبيق هو قانون مكان تواجد المستخدم؟ أم مكان استضافة البيانات؟ أم مكان الشركة المعالجة؟

4. معايير تحديد القانون الواجب التطبيق:

- في الاتحاد الأوروبي، على سبيل المثال، تنص GDPR على أن القانون الواجب التطبيق هو قانون الدولة التي يقيم فيها الشخص الذي تخصه البيانات، حتى لو كانت الشركة تقع في دولة أخرى.
- غالبًا ما يُستخدم معيار **مكان إقامة الفرد** أو **مكان المعالجة الرئيسية للبيانات** لتحديد القانون.
- بعض الاتفاقيات الثنائية أو متعددة الأطراف قد تحدد قواعد خاصة لتجاوز تعقيدات تنازع القوانين.

5. معايير تحديد الاختصاص القضائي:

- يمكن أن تكون هناك اختصاصات متعددة، مثل محكمة مكان إقامة صاحب البيانات، أو المحكمة في بلد الشركة التي تعالج البيانات.
- بعض القوانين تعطي الحق للأفراد برفع القضايا في محاكمهم المحلية حتى لو كانت الشركة خارج

[11] علاء عيد طه، الحماية القانونية للأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وتداولها، دراسة في ضوء اللائحة التنظيمية رقم 2016/679 الصادرة عن البرلمان والمجلس الأوروبي، مجلة كلية الحقوق للبحوث القانونية والاقتصادية، ع2، 2019.

حدود الدولة.

- التعاون الدولي ضروري لحل النزاعات العابرة للحدود، مثل تبادل الأدلة أو تنفيذ الأحكام.

6. الحلول القانونية:

- **الاتفاقيات الدولية:** تسعى لتوحيد قواعد الاختصاص وتنازع القوانين، مثل اتفاقيات التعاون القضائي.
- **مبدأ كفاية الحماية: (Adequacy)** حيث تعتمد دول على دول أخرى فقط إذا اعتبرت أن نظام حماية البيانات فيها كافٍ.
- **آليات التنسيق بين الجهات التنظيمية:** لضمان تنفيذ القوانين بشكل متكامل وعدم التعارض[12].

خلاصة:

تنازع القوانين والاختصاص القضائي في قضايا حماية البيانات يمثلان من أكبر التحديات في عصر العولمة الرقمية. وتتطلب هذه القضايا حلولًا دولية متناسقة، مع احترام سيادة الدول وحقوق الأفراد، لضمان حماية فعالة للبيانات الشخصية عبر الحدود.

المبحث السادس: الحلول القانونية لحماية البيانات عبر الحدود

1. الاتفاقيات الدولية والتنسيق بين الدول:

- **اتفاقية مجلس أوروبا رقم 108: (Convention 108)** أول اتفاقية دولية ملزمة تحكم حماية البيانات الشخصية، وتضع إطارًا قانونيًا للتعاون بين الدول.
- **الاتفاقيات الثنائية والمتعددة الأطراف[13]:** تبرم الدول اتفاقيات لتنظيم تبادل البيانات، وضمان تطبيق معايير حماية مشتركة.
- **مبادئ منظمة التعاون الاقتصادي والتنمية: (OECD)** تعمل على تنسيق المبادئ العامة لحماية البيانات وتسهيل تدفق البيانات بشكل آمن.

2. مبدأ كفاية الحماية: (Adequacy Decision)

- تعتمد بعض الدول، مثل الاتحاد الأوروبي، على مبدأ **كفاية الحماية**، حيث تسمح بنقل البيانات

[12] عمار ياسر محمد زهير البابلي، توظيف تقنيات الذكاء الاصطناعي في العمل الأمني، دراسة تطبيقية، مجلة الأمن والقانون، مج28، ع1، 2020.
[13] مجدي الداغر، اتجاهات النخبة نحو توظيف الإعلام الأمني لتطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وانعكاساته على دعم وتعزيز الأمن السيبراني في مصر، المجلة العربية لبحوث الإعلام والاتصال، ع33، ابريل/يونيو 2021.

فقط إلى الدول التي تقدم مستوى حماية يعادل ما هو معمول به في الاتحاد.

- مثال: تصنيف الاتحاد الأوروبي لبعض الدول مثل اليابان وكندا بأنها توفر حماية كافية، مما يسهل نقل البيانات إليها دون عقبات قانونية.

3. العقود والضمانات القانونية:

- **بنود حماية البيانات: (Standard Contractual Clauses -SCCs)** تستخدم هذه البنود في العقود بين الجهات التي تنقل البيانات عبر الحدود لضمان التزام الطرف المستقبل بمعايير حماية البيانات.
- **المبادئ التنظيمية للشركات: (Binding Corporate Rules -BCRs)** قواعد داخلية تلتزم بها الشركات متعددة الجنسيات لمعالجة البيانات عبر فروعها في دول مختلفة بشكل آمن ومتوافق مع القوانين.

4. التشريعات الوطنية المتوافقة مع المعايير الدولية:

- دول كثيرة تعمل على تحديث قوانينها لتتوافق مع المعايير الدولية مثل GDPR، مما يسهل عمليات تبادل البيانات الدولية ويقلل من التعارضات القانونية.

5. التعاون والتنفيذ القضائي الدولي:

- إنشاء آليات تعاون بين هيئات حماية البيانات في الدول المختلفة، لتبادل المعلومات، والتنسيق في التحقيقات، وتنفيذ الأحكام القضائية المتعلقة بحماية البيانات.
- مبادرات مثل **مجموعة عمل حماية البيانات الأوروبية** التي تعمل على تطبيق مشترك للقواعد عبر الدول الأعضاء[14].

6. استخدام التكنولوجيا لتأمين البيانات:

- توظيف تقنيات التشفير، والتجزئة، وإخفاء الهوية عند نقل البيانات عبر الحدود، مع وضع قواعد قانونية تحكم استخدام هذه التقنيات لضمان حماية البيانات.

خلاصة:

حماية البيانات الشخصية عند انتقالها عبر الحدود تتطلب إطارًا قانونيًا متكاملاً يجمع بين الاتفاقيات

[14] محمد أحمد المعداوي، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع الواصل الاجتماعي، دراسة مقارنة، مجلة كلية الشريعة والقانون، جامعة طنطا، مج33، ع4، ديسمبر 2018.

الدولية، المبادئ التعاقدية، التشريعات الوطنية المتوافقة، والتعاون القضائي بين الدول، بالإضافة إلى دعمها بتقنيات أمنية متطورة.

المبحث السابع: التزامات الشركات تجاه الأفراد

1. الشفافية والإخطار:

- يجب على الشركات إبلاغ الأفراد بشكل واضح ومفصل عن جمع بياناتهم، والأغراض التي ستُستخدم فيها، والجهات التي ستُشارك معها البيانات[15].
- توفير سياسة خصوصية واضحة وسهلة الوصول.

2. الحصول على الموافقة الصريحة:

- قبل جمع أو معالجة البيانات الشخصية، يجب الحصول على موافقة صريحة ومحددة من الأفراد، خاصة عند التعامل مع البيانات الحساسة.
- يجب أن تكون الموافقة طوعية وقابلة للسحب في أي وقت.

3. حماية البيانات وأمانها:

- اتخاذ التدابير التقنية والتنظيمية المناسبة لحماية البيانات من الاختراق، الفقدان، أو التلاعب.
- استخدام تقنيات مثل التشفير، التحكم في الوصول، وأنظمة الكشف عن التسلل.

4. الحق في الوصول والتصحيح:

- تمكين الأفراد من الاطلاع على بياناتهم الشخصية التي تحتفظ بها الشركة.
- السماح لهم بطلب تصحيح أي معلومات غير دقيقة أو ناقصة.

5. الحق في حذف البيانات ("الحق في النسيان")

- منح الأفراد الحق في طلب حذف بياناتهم الشخصية في ظروف معينة، مثل انتهاء الغرض من جمع البيانات أو سحب الموافقة.

6. تقييد المعالجة والاعتراض:

- تمكين الأفراد من تقييد استخدام بياناتهم أو الاعتراض على معالجتها لأسباب مشروعة.

[15] محمد حماد مرهج الهيتي، البحث عن حماية جنائية للبيانات والمعلومات الشخصية الإسمية المخزنة في الحاسب الآلي، مجلة كلية الشريعة والقانون، الإمارات، ع27، يوليو 2016.

7. إشعار خرق البيانات:

- في حال حدوث أي خرق أمني يؤثر على بيانات الأفراد، يجب إعلامهم بسرعة مع توضيح طبيعة الخرق والإجراءات المتخذة للتعامل معه.

8. تعيين مسؤول حماية البيانات:

- في بعض الحالات، يجب على الشركات تعيين مسؤول مختص بحماية البيانات لضمان الامتثال للقوانين وحماية حقوق الأفراد.

9. عدم نقل البيانات دون ضمانات كافية:

- عدم نقل بيانات الأفراد إلى جهات خارجية أو دول أخرى إلا بعد التأكد من وجود حماية كافية وفقًا للقوانين المعمول بها[16].

خلاصة:

التزامات الشركات تجاه الأفراد تهدف إلى احترام حقوقهم في الخصوصية، وضمان أن معالجة البيانات تتم بشفافية وأمان، مع إعطائهم السيطرة على بياناتهم الشخصية.

المبحث الثامن: المسؤولية القانونية والعقوبات المترتبة على الإخلال

1. المسؤولية القانونية:

هي الالتزام القانوني الذي يقع على الفرد أو الجهة عند مخالفة القوانين أو الأنظمة المعمول بها. تُعنى بتحمل عواقب الأفعال التي تخالف القانون، سواء كانت أفعالًا إيجابية (كالفعل الضار) أو سلبية (كالامتناع عن أداء واجب)[17].

2. أنواع المسؤولية القانونية:

- **المسؤولية المدنية:** تكون عادة لتعويض الضرر الذي يلحق بشخص أو ممتلكات نتيجة الإخلال.
- **المسؤولية الجنائية:** تتعلق بارتكاب جرائم أو مخالفات تستوجب عقوبات جنائية مثل الغرامات أو السجن.

[16] محمد ساي عبدالصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحقفي الخصوصية، دار النهضة العربية، القاهرة، 2016.
[17] محمود سلامة عبدالمنعم الشريف، الطبيعة القانونية للتنبؤ بالجريمة بواسطة الذكاء الاصطناعي ومشروعيته، المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي، مج3، 2021.

- **المسؤولية التأديبية:** خاصة بالعاملين في المؤسسات الحكومية أو الخاصة، وتُعنى بمخالفة اللوائح الداخلية.

3. العقوبات المترتبة على الإخلال:

تختلف العقوبات حسب نوع المخالفة وقوانين البلد، ومن أشهرها:

- **الغرامات المالية:** دفع مبلغ مالي كتعويض أو عقوبة.
- **السجن أو الحبس:** لفترة محددة حسب جسامة الجريمة.
- **التعويض المدني:** تعويض المتضرر عن الأضرار التي لحقت به.
- **الإيقاف أو الفصل التأديبي:** خاصة في الوظائف العامة أو المؤسسات.
- **حجز الممتلكات أو المنع من ممارسة نشاط معين.**

4. أمثلة على الإخلال والمسؤولية:

- مخالفة قوانين المرور تؤدي إلى غرامة أو حجز رخصة القيادة.
- التسبب في حادث نتيجة الإهمال يؤدي إلى تعويض المتضررين وربما عقوبات جنائية.
- الإخلال بالعقود يؤدي إلى مطالبات تعويضية في المحاكم المدنية.

كما تعني المسؤولية الجنائية:

- **التعريف:** هي مسؤولية الشخص أمام القانون الجنائي نتيجة ارتكابه فعلًا يُعد جريمة. الهدف منها حماية المجتمع من الأفعال الضارة أو الخطرة.
- **أمثلة على الجرائم:** السرقة، القتل، الاحتيال، الاعتداء، المخدرات.
- **العقوبات الجنائية:**

- **السجن:** لفترات متفاوتة حسب الجريمة.

- **الغرامات المالية:** تُفرض كعقوبة مالية.

- **العقوبات التكميلية:** مثل منع مزاولة مهنة معينة، أو الحبس الاحتياطي.

- **الإعدام:** في بعض البلدان وللجرائم الخطيرة جداً.

- **شروط المسؤولية الجنائية:** وجود فعل محظور (جريمة)، نية إجرامية (قصد)، وغياب مبررات شرعية (مثل الدفاع عن النفس)[18].

المسؤولية المدنية:

- **التعريف:** مسؤولية الشخص تجاه الآخرين بسبب الإضرار بهم أو بممتلكاتهم. الهدف هو تعويض المتضرر وليس العقاب.
- **أمثلة:** تعويض عن حادث سيارة، تعويض عن ضرر ناتج عن إهمال طبي.
- **أنواع الأضرار:**

- **المادية:** خسائر مالية مثل تلف ممتلكات.

- **المعنوية:** ألم نفسي أو تشويه السمعة.

- **العقوبات /التدابير:**

- دفع تعويض مالي للمتضرر.

- إعادة الحالة إلى ما كانت عليه إذا أمكن (مثل إصلاح ممتلكات).

- **شروط المسؤولية المدنية:** وجود ضرر، خطأ أو إهمال، وعلاقة سببية بين الخطأ والضرر.

المسؤولية التأديبية:

- **التعريف:** مسؤولية الموظف أو العامل أمام جهة عمله بسبب مخالفة الأنظمة واللوائح الداخلية.
- **أمثلة:** التأخير المتكرر، عدم تنفيذ التعليمات، السلوك غير المهني.
- **الجزاءات التأديبية:**

- توجيه إنذار شفوي أو كتابي.

- خصم جزء من الراتب.

- الإيقاف عن العمل مؤقتًا.

- الفصل من العمل.

[18] محمود عبدالعظيم، بيزنس البيانات الشخصية يغزو السوق المصرية، جريدة الاتحاد الإماراتية بتاريخ 8 يناير، 2026.

- **الهدف:** الحفاظ على النظام والانضباط داخل المؤسسة وتحسين الأداء[19].

الخاتمة

في ظل التطور التقني المتسارع واعتماد الشركات والمؤسسات والأفراد على الوسائل الرقمية في تخزين ومعالجة البيانات، أصبحت حماية البيانات الشخصية ضرورة ملحة لضمان الخصوصية والأمن الرقمي. إن حماية البيانات الشخصية ليست مجرد التزام قانوني بل حق أساسي من حقوق الإنسان يعزز الثقة بين الأطراف المعنية ويُسهم في استقرار الأعمال والتعاملات الدولية[20].

تؤكد المعايير الدولية مثل **اللائحة العامة لحماية البيانات (GDPR)** الصادرة عن الاتحاد الأوروبي، وأحكام القانون الدولي الخاص، على أهمية وضع إطار قانوني متكامل وفعال لحماية البيانات، يتضمن شفافية في المعالجة، وضمان حقوق الأفراد، وتطبيق عقوبات مناسبة على المخالفين.

التوصيات

1. **تبني سياسات واضحة لحماية البيانات:** على الشركات والمؤسسات وضع سياسات وإجراءات صارمة تتماشى مع المعايير الدولية مثل GDPR، تشمل جمع البيانات، تخزينها، معالجتها، ومشاركتها.
2. **التوعية والتدريب:** تعزيز ثقافة حماية البيانات بين العاملين من خلال برامج تدريبية دورية، لضمان فهمهم للمخاطر وسبل الحماية.
3. **تعيين مسؤول حماية البيانات: (DPO)** تعيين موظف مختص يكون مسؤولاً عن مراقبة تطبيق سياسات حماية البيانات والتواصل مع الجهات الرقابية.
4. **تنفيذ تقنيات أمنية متقدمة:** استخدام تقنيات التشفير، وأنظمة الحماية الإلكترونية، والنسخ الاحتياطية لضمان سلامة البيانات.
5. **الالتزام بمبادئ الشفافية:** إعلام الأفراد بشكل واضح عن كيفية جمع بياناتهم واستخدامها وحقوقهم المتعلقة بها.
6. **التعاون الدولي:** التنسيق مع الجهات القانونية والرقابية الدولية لضمان توافق الإجراءات مع

[19] محمود عبدالرحمن، التطورات الحديثة لمفهوم الحق في الخصوصية – الحق في الخصوصية المعلوماتية، مجلة كلية القانون الكويتية العالمية، ع9، س3، مارس 2015.

[20] منى تركي الموسوي، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها، مجلة كلية بغداد للعلوم الاقتصادية – عدد خاص بمؤتمر الكلية، جامعة بغداد، 2013.

القانون الدولي الخاص، خاصة في حال تبادل البيانات عبر الحدود.

7. **مراجعة دورية:** إجراء مراجعات دورية للسياسات والإجراءات لضمان استمرارية التوافق مع التشريعات الحديثة والتقنيات الجديدة.

المصادر والمراجع

مصادر ومراجع أساسية:

1. أشرف جابر سيد، الجوانب القانونية لمواقع التواصل الاجتماعي، دار النهضة العربية، القاهرة، 2013.
2. باسل فايز حمد القطاطشة، ممدوح حسن العدوان، الحماية الجنائية لخصوصية البيانات الشخصية الرقمية، دراسة مقارنة، رسالة دكتوراه، جامعة العلوم الإسلامية، عمان، 2022.
3. بوكر رشيدة، تحديات العصر في مواجهة خطط حماية الحق في الخصوصية، مجلة حقوق الإنسان والحريات العامة، مج7، ع2، 2022.
4. رانيا سليمان أبو المعاطي محمود، ونهي محمد ابراهيم الدسوقي، وفاتن فايز حميدة الصفتي، سياسة مكافحة الإرهاب الإلكتروني، مصر والسعودية أنموذجاً، المركز العربي للبحوث والدراسات، آفاق سياسية، ع53، 2020.
5. سليم محمد سليم حسين، الحماية الجنائية للبيانات الشخصية المعالجة آلياً، دراسة مقارنة، مجلة العلوم القانونية والاقتصادية، كلية الحقوق جامعة عين شمس، مج62، ع1، 2020.
6. شلواح ميرة، بشيري كهينة، المسؤولية المدنية عن انتهاك حق الخصوصية في المجال الرقمي، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة عبدالرحمان ميرة، بجاية، 2019-2020.
7. طارق جمعه السيد راشد، الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي، دراسة مقارنة، مجلة القانون والاقتصاد، كلية الحقوق، جامعة القاهرة، ملحق خاص، ع92، بدون سنة.
8. طارق جمعه السيد راشد، الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي، دراسة مقارنة، مجلة القانون والاقتصاد، كلية الحقوق، جامعة القاهرة، ملحق خاص، ع92، بدون سنة.
9. عزت عبدالمحسن ابراهيم، الحق في الخصوصية الرقمية وتحديات عصر التقنية، مجلة العلوم

القانونية والاقتصادية، كلية الحقوق، جامعة عين شمس، مج62، ع1، 2020.

10. علاء الدين عبدالله فواز الخصاونة، الحماية القانونية للخصوصية والبيانات الشخصية في نطاق المعلوماتية، مجلة جامعة الشارقة للعلوم الشرعية والقانونية، جامعة الشارقة، مج8، ع2، 2011.

11. علاء عيد طه، الحماية القانونية للأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وتداولها، دراسة في ضوء اللائحة التنظيمية رقم 2016/679 الصادرة عن البرلمان والمجلس الأوروبي، مجلة كلية الحقوق للبحوث القانونية والاقتصادية، ع2، 2019.

12. عمار ياسر محمد زهير البابلي، توظيف تقنيات الذكاء الاصطناعي في العمل الأمني، دراسة تطبيقية، مجلة الأمن والقانون، مج28، ع1، 2020.

13. مجدي الداغر، اتجاهات النخبة نحو توظيف الإعلام الأمني لتطبيقات الذكاء الاصطناعي في مكافحة الجرائم الإلكترونية وانعكاساته على دعم وتعزيز الأمن السيبراني في مصر، المجلة العربية لبحوث الإعلام والاتصال، ع33، ابريل/يونيو 2021.

14. محمد أحمد المعداوي، حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع الواصل الاجتماعي، دراسة مقارنة، مجلة كلية الشريعة والقانون، جامعة طنطا، مج33، ع4، ديسمبر 2018.

15. محمد حماد مرهج الهيتي، البحث عن حماية جناية للبيانات والمعلومات الشخصية الإسمية المخزنة في الحاسب الآلي، مجلة كلية الشريعة والقانون، الإمارات، ع27، يوليو 2016.

16. محمد سامي عبدالصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحقفي الخصوصية، دار النهضة العربية، القاهرة، 2016.

17. محمود سلامة عبدالمنعم الشريف، الطبيعة القانونية للتنبؤ بالجريمة بواسطة الذكاء الاصطناعي ومشروعيته، المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي، مج3، 2021.

18. محمود عبدالعظيم، بيزنس البيانات الشخصية يغزو السوق المصرية، جريدة الاتحاد الإماراتية بتاريخ 8 يناير، 2026.

19. محمود عبدالرحمن، التطورات الحديثة لمفهوم الحق في الخصوصية – الحق في الخصوصية المعلوماتية، مجلة كلية القانون الكويتية العالمية، ع9، س3، مارس 2015.

20. منى تركي الموسوي، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها، مجلة كلية بغداد للعلوم الاقتصادية – عدد خاص بمؤتمر الكلية، جامعة بغداد، 2013.

21. اللائحة العامة لحماية البيانات- (GDPR) الاتحاد الأوروبي.

22. الاتفاقية رقم 108 لحماية البيانات الشخصية -المجلس الأوروبي.

23. قانون حماية البيانات الشخصية في السعودية (PDPL).

24. California Consumer Privacy Act (CCPA) الولايات المتحدة الأمريكية.

تقارير وأبحاث:

1. تقارير سنوية من شركات مثل **PwC, Deloitte, KPMG** حول حماية البيانات وأمن المعلومات.

2. أبحاث ودراسات من **هيئة الإنترنت العالمية** ومنظمات حقوق الإنسان المتعلقة بالخصوصية.