الخصوصية وحماية البيانات في عصر الذكاء الاصطناعي التوليدي

دراسة أكاديمية في الجوانب التقنية والقانونية والأخلاقية

المؤلف
الأستاذ أسامة المحارمة

المؤلف
د. زيد الربابعة

تحت إشراف وإدارة
نادي الليونز رويال سوردز – عمان
LIONS ROYAL SWORDS CLUB – AMMAN

الخصوصية وحماية البيانات في عصر الذكاء الاصطناعي التوليدي

دراسة أكاديمية في الجوانب التقنية والقانونية والأخلاقية

المؤلف والباحث الاول

د. زيد الربابعة

المؤلف الثاني

ا. أسامة المحارمة

رقم الإيداع لدى دائرة المكتبة الوطنية

(2026/6/3708)

بيانات الفهرسة الأولية للكتاب:

- **عنوان الكتاب :**الخصوصية وحماية البيانات في عصر الذكاء الاصطناعي التوليدي: دراسة أكاديمية في الجوانب التقنية والقانونية والأخلاقية
- **إعداد :**ربابعه، زيد محمد علي خليل
- **إعداد (آخرون) :**المحارمه، اسامه خالد عبد الكريم.
- **بيانات النشر :**عمان: زيد محمد علي خليل ربابعه، 2026
- **الوصف المادي** 138 **:**صفحة.
- **رقم التصنيف** 343.099
- **الواصفات/ :**حماية البيانات//الأمن السيبراني//الذكاء الاصطناعي//الاتصالات الرقمية//المؤسسات//التشريعات الدولية/
- **الطبعة :**الطبعة الأولى

يتحمل المؤلف كامل المسؤولية القانونية عن محتوى مصنفه ولا يعبر هذا المصنف عن رأي دائرة المكتبة الوطنية أو أي جهة حكومية أخرى

كلمة شكر وتقدير

Amman Royal Swords
LIONS CLUB

الحمد لله الذي بنعمته تتم الصالحات، والصلاة والسلام على سيدنا محمد وعلى آله وصحبه أجمعين.

تم إعداد وتجميع هذه الدراسة تحت إشراف ودعم **نادي الليونز رويال سوردز – عمان**، الذي وفر البيئة المناسبة والداعمة لإنجاز هذا العمل العلمي والمعرفي.

وأتقدم بخالص الشكر والتقدير إلى الأستاذ الليون **أسامة المحارمة**، قائد النادي، لما قدمه من دعم متواصل وتشجيع حقيقي خلال مراحل إعداد هذه الدراسة. فقد كان له دور بارز في تسهيل العمل، والمساهمة في جمع بعض المعلومات والمراجع، وتوفير كل ما يلزم لإنجاح هذا المشروع، الأمر الذي كان له أثر كبير في إخراج هذه الدراسة بالصورة التي تليق بأهدافها ورسالتها.

كما أتوجه بالشكر والامتنان إلى إدارة وأعضاء **نادي الليونز رويال سوردز – عمان** على إيمانهم بأهمية المعرفة والتطوير المستمر، وعلى إتاحة الفرصة لي للانطلاق والعمل من خلال **لجنة الذكاء الاصطناعي** التابعة للنادي، مما أتاح المجال لتحويل الأفكار والطموحات إلى مبادرات ومشاريع معرفية تسهم في نشر الوعي وتعزيز الاستخدام المسؤول للتقنيات الحديثة.

إن هذا العمل ما كان ليرى النور بعد توفيق الله سبحانه وتعالى لولا الجهود المخلصة والتعاون البناء والدعم الذي حظيت به من النادي وأعضائه، ولذلك فإن هذه الصفحة تمثل رسالة شكر ووفاء وتقدير لكل من ساهم، بصورة مباشرة أو غير مباشرة، في إنجاز هذه الدراسة.

مع خالص الاحترام والتقدير،

د. زيد الربابعة
مؤلف الدراسة

المحتويات

الفصل الأول: مدخل إلى الذكاء الاصطناعي..... 6
الفصل الثاني: البيانات والاقتصاد الرقمي..... 12
الفصل الثالث: الخصوصية الرقمية..... 17
الفصل الرابع: البيانات الشخصية..... 22
الفصل الخامس: مبادئ حماية البيانات الشخصية..... 27
الفصل السادس: إدارة دورة حياة البيانات الشخصية..... 33
الفصل السابع: مخاطر البيانات الشخصية والتهديدات الأمنية في العصر الرقمي..... 38
الفصل الثامن: الأمن السيبراني وحماية البيانات الشخصية..... 44
الفصل التاسع: الإطار القانوني لحماية البيانات الشخصية..... 51
الفصل العاشر: اللائحة العامة لحماية البيانات الأوروبية(GDPR) 57
الفصل الحادي عشر: قانون حماية البيانات الشخصية الأردني رقم (24) لسنة 2023 .. 64
الفصل الثاني عشر: نظام حماية البيانات الشخصية السعودي (PDPL) والتشريعات العربية المقارنة..... 72
الفصل الثالث عشر: قانون خصوصية المستهلك في كاليفورنيا (CCPA/CPRA) والتشريعات الأمريكية لحماية البيانات..... 79
الفصل الرابع عشر: قانون الذكاء الاصطناعي الأوروبي(EU AI Act) 85
الفصل الخامس عشر: أخلاقيات الذكاء الاصطناعي وحماية البيانات..... 91
الفصل السادس عشر: حوكمة الذكاء الاصطناعي وإدارة الامتثال المؤسسي..... 97
الفصل السابع عشر: الخصوصية وحماية البيانات في ChatGPT و Claudeو Geminiو Copilot 103
الفصل الثامن عشر: النماذج المحلية للذكاء الاصطناعي (Local AI Models) وحماية البيانات 110
الفصل التاسع عشر: الخصوصية وحماية البيانات في الحوسبة السحابية..... 115
الفصل العشرون: إدارة الحوادث واختراقات البيانات الشخصية..... 122
الملاحق..... 128
الملحق الثاني: قائمة الاختصارات..... 130
الملحق الثالث: نماذج قانونية..... 132
الملحق الرابع: المراجع العربية..... 134
الملحق الخامس: المراجع الأجنبية..... 135

الفصل الأول: مدخل إلى الذكاء الاصطناعي

يُعد الذكاء الاصطناعي (Artificial Intelligence - AI) أحد أهم التطورات التقنية التي شهدها القرن الحادي والعشرون، إذ أصبح جزءاً أساسياً من مختلف جوانب الحياة اليومية والاقتصادية والعلمية. وقد أدى التقدم المتسارع في قدرات الحوسبة وتوافر البيانات الضخمة إلى انتقال الذكاء الاصطناعي من كونه مجالاً بحثياً محدوداً إلى تقنية محورية تؤثر في القرارات الاقتصادية والصناعية والتعليمية والطبية والأمنية.

وفي السنوات الأخيرة، شهد العالم طفرة غير مسبوقة مع ظهور نماذج الذكاء الاصطناعي التوليدي، القادرة على إنتاج النصوص والصور والصوت والفيديو بدرجات عالية من الواقعية، مما فتح آفاقاً جديدة للابتكار والإنتاجية، وفي الوقت ذاته أثار العديد من التساؤلات المتعلقة بالخصوصية وحماية البيانات والأبعاد القانونية والأخلاقية لهذه التقنيات.

يهدف هذا الفصل إلى تقديم أساس نظري لفهم الذكاء الاصطناعي، من خلال استعراض تطوره التاريخي، والتمييز بين أنواعه المختلفة، وشرح مفاهيم التعلم الآلي والتعلم العميق، وصولاً إلى نماذج اللغة الكبيرة التي تمثل العمود الفقري لمعظم تطبيقات الذكاء الاصطناعي التوليدي الحديثة.

تطور الذكاء الاصطناعي

البدايات الفكرية للذكاء الاصطناعي

يرجع مفهوم الذكاء الاصطناعي إلى محاولات الإنسان القديمة لفهم طبيعة التفكير البشري ومحاكاته. وقد ظهرت أفكار أولية حول الآلات الذكية في الفلسفة اليونانية القديمة، إلا أن التطبيق العملي لم يبدأ إلا مع ظهور الحواسيب الحديثة في القرن العشرين.

في عام 1950 نشر عالم الرياضيات البريطاني Alan Turingورقته العلمية الشهيرة "Computing Machinery and Intelligence"، والتي طرح فيها سؤالاً أصبح محورياً في هذا المجال: "هل تستطيع الآلات أن تفكر؟". كما قدم اختبار تورينغ(Turing Test) ، الذي يهدف إلى قياس قدرة الآلة على محاكاة السلوك الذكي للإنسان.

وفي عام 1956 عُقد مؤتمر دارتموث في الولايات المتحدة، والذي يُعد نقطة الانطلاق الرسمية لعلم الذكاء الاصطناعي. خلال هذا المؤتمر استخدم مصطلح "Artificial Intelligence" لأول مرة من قبل الباحث John McCarthy، الذي يُعرف اليوم بأحد الآباء المؤسسين للذكاء الاصطناعي.

مراحل تطور الذكاء الاصطناعي

المرحلة الأولى: الأنظمة الرمزية(1956 – 1980)

اعتمدت الأنظمة الأولى للذكاء الاصطناعي على القواعد المنطقية والرموز الرياضية. وكان الهدف بناء أنظمة قادرة على محاكاة التفكير البشري من خلال قواعد محددة مسبقاً.

ومن أبرز خصائص هذه المرحلة: الاعتماد على قواعد "إذا-فإن" (IF-THEN) والحاجة إلى خبراء بشريين لكتابة المعرفة ومحدودية القدرة على التعلم الذاتي وضعف الأداء في البيئات المعقدة.

ومن أشهر تطبيقات هذه المرحلة الأنظمة الخبيرة(Expert Systems) ، التي استخدمت في المجالات الطبية والهندسية.

المرحلة الثانية: شتاء الذكاء الاصطناعي

رغم التفاؤل الكبير في العقود الأولى، واجه الباحثون تحديات كبيرة بسبب محدودية قدرات الحواسيب وقلة البيانات المتاحة. وأدى ذلك إلى تراجع التمويل والاهتمام البحثي فيما عُرف باسم "شتاء الذكاء الاصطناعي.(AI Winter) "

شهدت هذه الفترة: انخفاض الاستثمارات وفشل العديد من المشاريع وتراجع التوقعات المتفائلة.

المرحلة الثالثة: التعلم الآلي(1990 – 2010)

بدأت مرحلة جديدة مع تطور قدرات الحوسبة وتوافر كميات أكبر من البيانات. وبدلاً من برمجة جميع القواعد يدوياً، أصبح بالإمكان تدريب الأنظمة على التعلم من البيانات.

ومن أبرز إنجازات هذه المرحلة: تطوير خوارزميات التصنيف والتنبؤ واستخدام الشبكات العصبية الحديثة وظهور تطبيقات التعرف على الصور والكلام.

المرحلة الرابعة: عصر التعلم العميق (2010 – حتى الآن)

شهد العقد الأخير طفرة كبيرة نتيجة توافر: البيانات الضخمة (Big Data) والمعالجات الرسومية (GPUs) والخوارزميات المتقدمة.

وأدى ذلك إلى تحسين أداء الأنظمة الذكية بشكل غير مسبوق، خصوصاً في: الرؤية الحاسوبية ومعالجة اللغة الطبيعية والترجمة الآلية والمركبات ذاتية القيادة.

الذكاء الاصطناعي التقليدي والذكاء الاصطناعي التوليدي

الذكاء الاصطناعي التقليدي

يشير الذكاء الاصطناعي التقليدي إلى الأنظمة المصممة لتنفيذ مهام محددة اعتماداً على تحليل البيانات أو تطبيق قواعد محددة مسبقاً.

ومن أمثلته: أنظمة كشف الاحتيال البنكي وأنظمة التوصية وأنظمة التنبؤ بالمبيعات وبرامج التعرف على الوجوه.

يتميز هذا النوع بما يلي: يركز على اتخاذ القرار أو التصنيف وينتج مخرجات محددة مسبقاً ولا ينشئ محتوى جديداً بشكل مستقل.

الذكاء الاصطناعي التوليدي

الذكاء الاصطناعي التوليدي (Generative AI) هو مجموعة من النماذج القادرة على إنشاء محتوى جديد بناءً على البيانات التي تدربت عليها.

ويشمل ذلك: النصوص والصور والفيديو والصوت والبرمجيات.

ومن أشهر الأمثلة:

- ChatGPT
- Claude
- Gemini
- Microsoft Copilot

خصائص الذكاء الاصطناعي التوليدي

إنتاج محتوى جديد وفهم السياق اللغوي ودعم التفاعل الطبيعي مع المستخدم والقدرة على التكيف مع مهام متعددة.

التعلم الآلي والتعلم العميق

مفهوم التعلم الآلي

التعلم الآلي (Machine Learning) هو فرع من فروع الذكاء الاصطناعي يركز على تطوير أنظمة قادرة على التعلم من البيانات دون الحاجة إلى برمجة صريحة لكل حالة.

بدلاً من كتابة القواعد يدوياً، يتم تزويد النظام ببيانات تدريبية ليستخلص الأنماط والعلاقات بنفسه.

أمثلة :التنبؤ بأسعار العقارات وتصنيف الرسائل المزعجة واكتشاف الاحتيال المالي وتحليل سلوك العملاء.

أنواع التعلم الآلي

التعلم الموجّه(Supervised Learning)

يستخدم بيانات تحتوي على مدخلات ومخرجات معروفة مسبقاً وأمثلة: تصنيف البريد الإلكتروني والتنبؤ بالأسعار.

التعلم غير الموجّه(Unsupervised Learning)

يعتمد على اكتشاف الأنماط دون وجود إجابات مسبقة وأمثلة: تقسيم العملاء إلى مجموعات وتحليل السلوك الشرائي.

التعلم بالتعزيز(Reinforcement Learning)

يتعلم النظام من خلال التجربة والخطأ والحصول على مكافآت أو عقوبات وأمثلة: الألعاب الإلكترونية والروبوتات والمركبات الذاتية القيادة.

التعلم العميق

التعلم العميق (Deep Learning) هو فرع متقدم من التعلم الآلي يعتمد على الشبكات العصبية الاصطناعية متعددة الطبقات.

يحاكي هذا الأسلوب طريقة عمل الخلايا العصبية في الدماغ البشري بصورة مبسطة.

ومن أبرز استخداماته: التعرف على الصور والتعرف على الصوت والترجمة الآلية وتحليل النصوص والذكاء الاصطناعي التوليدي.

لماذا أحدث التعلم العميق ثورة تقنية؟

ساهمت ثلاثة عوامل رئيسية في نجاح التعلم العميق: توفر البيانات الضخمة وتطور قدرات المعالجة الرسومية وتطوير خوارزميات أكثر كفاءة.

وقد مكنت هذه العوامل الأنظمة من تحقيق مستويات أداء تقترب من الأداء البشري في العديد من المهام.

ما هي نماذج اللغة الكبيرة؟

نماذج اللغة الكبيرة (Large Language Models - LLMs) هي نماذج ذكاء اصطناعي تعتمد على الشبكات العصبية العميقة وتُدرّب على كميات هائلة من النصوص بهدف فهم اللغة البشرية وإنتاجها.

وتُعد هذه النماذج الأساس الذي تعتمد عليه معظم تطبيقات الذكاء الاصطناعي التوليدي الحديثة.

آلية عمل نماذج اللغة الكبيرة

تعتمد هذه النماذج على التنبؤ بالكلمة أو الرمز التالي ضمن تسلسل لغوي.

فعلى سبيل المثال، إذا كانت الجملة:

"تسعى المؤسسات إلى حماية"_____

فإن النموذج يحاول توقع الكلمة الأكثر احتمالاً مثل:

- البيانات
- المعلومات
- الخصوصية

ومع تكرار هذه العملية مليارات المرات أثناء التدريب، يطور النموذج قدرة متقدمة على فهم الأنماط اللغوية.

بنية المحولات**(Transformers)**

أحدثت بنية المحولات (Transformers) ثورة في مجال معالجة اللغة الطبيعية منذ تقديمها عام 2017.

وتتميز بـ: معالجة النصوص بكفاءة عالية وفهم العلاقات بين الكلمات ودعم السياقات الطويلة وقابلية التوسع إلى أحجام ضخمة ووتعتمد معظم النماذج الحديثة عليها.

أمثلة على نماذج اللغة الكبيرة

من أبرز النماذج المستخدمة عالمياً:

- GPT
- Claude
- Gemini

- Llama
- Qwen
- Mistral

وتستخدم هذه النماذج في: المساعدات الذكية والبحث والتحليل والبرمجة والتعليم وخدمة العملاء وإنشاء المحتوى.

خاتمة الفصل

شهد الذكاء الاصطناعي تطوراً متسارعاً منذ ظهوره في منتصف القرن العشرين، وانتقل من الأنظمة القائمة على القواعد إلى النماذج التوليدية المتقدمة القادرة على فهم اللغة الطبيعية وإنتاج محتوى متنوع بدرجة عالية من الكفاءة. وقد شكل التعلم الآلي والتعلم العميق الأساس العلمي لهذه الثورة التقنية، بينما أصبحت نماذج اللغة الكبيرة القلب النابض لمعظم تطبيقات الذكاء الاصطناعي الحديثة.

ويُعد فهم هذه المفاهيم أساسياً قبل الانتقال إلى دراسة الخصوصية وحماية البيانات، لأن طبيعة عمل هذه النماذج ترتبط بشكل مباشر بكيفية جمع البيانات ومعالجتها واستخدامها، وهو ما سيتم تناوله في الفصول اللاحقة.

الفصل الثاني: البيانات والاقتصاد الرقمي

مقدمة الفصل

أصبحت البيانات في القرن الحادي والعشرين مورداً استراتيجياً لا يقل أهمية عن الموارد الطبيعية التقليدية كالنفط والغاز والمعادن. وقد أدى التحول الرقمي المتسارع إلى جعل البيانات أساساً للابتكار والنمو الاقتصادي وصنع القرار في مختلف القطاعات. فالحكومات تعتمد على البيانات لتطوير السياسات العامة، والمؤسسات تستخدمها لتحسين العمليات والخدمات، بينما تستثمر شركات التكنولوجيا مليارات الدولارات في جمع البيانات وتحليلها واستثمارها تجارياً.

وفي ظل صعود الذكاء الاصطناعي التوليدي، ازدادت أهمية البيانات بشكل غير مسبوق، إذ تعتمد النماذج الذكية الحديثة على كميات هائلة من البيانات للتعلم والتطوير وتحسين الأداء. لذلك أصبح فهم طبيعة البيانات وقيمتها الاقتصادية وأنواعها المختلفة ضرورة أساسية لفهم التحديات المتعلقة بالخصوصية وحماية البيانات.

تعريف البيانات

البيانات (Data) هي مجموعة من الحقائق أو الأرقام أو الرموز أو النصوص أو الصور أو الأصوات التي تمثل معلومات أولية يمكن جمعها وتخزينها ومعالجتها واستخدامها لأغراض مختلفة.

وتشكل البيانات المادة الخام التي تُبنى عليها المعلومات والمعرفة واتخاذ القرار.

فعلى سبيل المثال:

العنصر	مثال
بيانات	35، 42، 50
معلومات	متوسط درجات الطلاب 42
معرفة	مستوى التحصيل الدراسي منخفض ويحتاج إلى تحسين

وبالتالي فإن البيانات وحدها لا تملك قيمة كبيرة ما لم يتم تنظيمها وتحليلها وتحويلها إلى معلومات قابلة للاستخدام.

الفرق بين البيانات والمعلومات والمعرفة

غالباً ما يحدث خلط بين هذه المفاهيم الثلاثة رغم اختلافها والبيانات (Data)حقائق خام غير معالجة.

مثال:

- اسم العميل
- رقم الهاتف
- العمر

المعلومات(Information) بيانات تم تنظيمها وتحليلها.

مثال: 70% من العملاء تتراوح أعمارهم بين 25 و40 عاماً والمعرفة (Knowledge)فهم واستنتاجات مبنية على المعلومات.

مثال :يجب توجيه الحملات التسويقية نحو الفئة العمرية الأكثر نشاطاً .

خصائص البيانات الجيدة

لكي تكون البيانات ذات قيمة حقيقية يجب أن تتمتع بعدد من الخصائص: الدقة (Accuracy)أن تكون خالية من الأخطاء والاكتمال (Completeness)أن تحتوي على جميع العناصر المطلوبة والحداثة (Timeliness)أن تكون محدثة ومتوافقة مع الواقع الحالي والاتساق (Consistency)عدم وجود تناقض بين البيانات المختلفة والموثوقية (Reliability)إمكانية الاعتماد عليها في اتخاذ القرار.

البيانات المنظمة

هي البيانات المخزنة في جداول وقواعد بيانات ذات هيكل محدد وقواعد بيانات العملاء وجداول المبيعات والسجلات المالية ووتتميز بسهولة البحث والتحليل والمعالجة.

البيانات شبه المنظمة

هي البيانات التي تحتوي على هيكل جزئي يسمح بتنظيمها بدرجات متفاوتة وملفات XML وملفات JSON ورسائل البريد الإلكتروني.

البيانات غير المنظمة

تمثل النسبة الأكبر من البيانات الرقمية في العالم والصور والفيديو والملفات الصوتية والمستندات النصية ومنشورات وسائل التواصل الاجتماعي.

وتتطلب تقنيات متقدمة لتحليلها واستخراج المعلومات منها.

مفهوم البيانات الشخصية

يقصد بالبيانات الشخصية أي معلومات تتعلق بشخص طبيعي يمكن التعرف عليه بشكل مباشر أو غير مباشر.

ومن الأمثلة: الاسم والرقم الوطني والبريد الإلكتروني ورقم الهاتف والعنوان والصورة الشخصية وتعد هذه البيانات محور معظم تشريعات حماية البيانات الحديثة.

البيانات الشخصية الحساسة

فئة خاصة تتطلب حماية مشددة، تشمل البيانات الصحية والبيومترية والجينية وغيرها، وتُفصَّل أنواعها وضوابطها القانونية في الفصل الرابع.

الهوية الرقمية

مجموعة البيانات التي تُعرِّف الفرد إلكترونياً، وتُعالَج بالتفصيل في الفصل الثالث ضمن مكوناتها والبصمة الرقمية وأثرها على الخصوصية.

مفهوم البيانات الضخمة

يقصد بالبيانات الضخمة مجموعات البيانات التي تتجاوز قدرات أنظمة المعالجة التقليدية من حيث الحجم أو السرعة أو التنوع.

وقد أصبحت البيانات الضخمة أحد أهم محركات الاقتصاد الرقمي الحديث.

خصائص البيانات الضخمة

تعرف البيانات الضخمة غالباً من خلال خمسة أبعاد رئيسية تعرف باسم (Vs5): الحجم (Volume)كميات هائلة من البيانات والسرعة (Velocity)تدفق البيانات بشكل مستمر وسريع والتنوع (Variety)اختلاف أشكال البيانات وأنواعها والموثوقية (Veracity)جودة البيانات وصحتها والقيمة (Value)القدرة على تحقيق فائدة اقتصادية أو تشغيلية.

مصادر البيانات الضخمة

تشمل: وسائل التواصل الاجتماعي والهواتف الذكية وأجهزة إنترنت الأشياء وأنظمة المؤسسات ومحركات البحث والمعاملات المالية والمستشعرات الصناعية.

مفهوم الاقتصاد الرقمي

الاقتصاد الرقمي هو الاقتصاد الذي تعتمد أنشطته بشكل أساسي على التكنولوجيا الرقمية والبيانات والشبكات الإلكترونية.

وقد أصبح يمثل نسبة متزايدة من الناتج المحلي الإجمالي للدول المتقدمة والنامية على حد سواء.

البيانات كأصل اقتصادي

في الماضي كانت قيمة الشركات ترتبط بالأصول المادية مثل: الأراضي والمصانع والمعدات.

أما اليوم فإن القيمة السوقية لكثير من الشركات تعتمد بشكل أساسي على: البيانات والبرمجيات والخوارزميات والملكية الفكرية.

ولهذا السبب يطلق بعض الباحثين على البيانات وصف: "نفط القرن الحادي والعشرين"

مع الإشارة إلى أن البيانات تختلف عن النفط في إمكانية إعادة استخدامها مرات غير محدودة دون استهلاكها.

نماذج الأعمال المعتمدة على البيانات

تقوم العديد من الشركات الحديثة على استثمار البيانات بشكل مباشر أو غير مباشر.

ومن الأمثلة: الإعلانات الرقمية تعتمد على تحليل سلوك المستخدمين وتخصيص المحتوى الإعلاني والتجارة الإلكترونية تستخدم البيانات لتوقع احتياجات العملاء وتحسين المبيعات والخدمات المالية تعتمد على البيانات لتقييم المخاطر وكشف الاحتيال والذكاء الاصطناعي تعتمد النماذج الذكية على البيانات في التدريب والتطوير.

العلاقة بين البيانات والذكاء الاصطناعي

لا يمكن للذكاء الاصطناعي أن يعمل بكفاءة دون بيانات.

فكل نموذج ذكاء اصطناعي يحتاج إلى: بيانات للتدريب وبيانات للاختبار وبيانات للتقييم والتحسين.

كلما كانت البيانات أكثر جودة وتنوعاً، زادت قدرة النموذج على تقديم نتائج دقيقة.

أهمية البيانات في نماذج الذكاء الاصطناعي التوليدي

تعتمد النماذج الحديثة على كميات ضخمة من البيانات تشمل: الكتب والمقالات والمواقع الإلكترونية والمستندات والأكواد البرمجية.

ومن خلال تحليل هذه البيانات تتعلم النماذج الأنماط اللغوية والمعرفية التي تمكنها من إنتاج محتوى جديد.

التحديات المرتبطة باستخدام البيانات

رغم الفوائد الكبيرة للبيانات، فإن استخدامها يثير العديد من التحديات: الخصوصية إمكانية الكشف عن معلومات شخصية والأمن تعرض البيانات للاختراق أو التسريب والتحيز احتمالية انتقال التحيزات الموجودة في البيانات إلى النماذج والملكية الفكرية إشكاليات استخدام المحتوى المحمي بحقوق النشر والامتثال القانوني ضرورة الالتزام بالتشريعات الوطنية والدولية.

مستقبل البيانات في عصر الذكاء الاصطناعي

تشير التقديرات إلى أن حجم البيانات العالمية سيستمر في النمو بمعدلات غير مسبوقة خلال العقود القادمة. ومع انتشار الذكاء الاصطناعي وإنترنت الأشياء والحوسبة السحابية، ستصبح البيانات أكثر ارتباطاً بجميع الأنشطة الإنسانية.

وفي المقابل، ستزداد أهمية التشريعات والسياسات التي تنظم جمع البيانات ومعالجتها واستخدامها، لضمان تحقيق التوازن بين الابتكار وحماية حقوق الأفراد.

خاتمة الفصل

تمثل البيانات الأساس الذي يقوم عليه الاقتصاد الرقمي والذكاء الاصطناعي الحديث. وقد أصبحت مورداً استراتيجياً يساهم في خلق القيمة الاقتصادية وتحسين الخدمات وتطوير الابتكار. إلا أن هذه الأهمية المتزايدة للبيانات تفرض مسؤوليات قانونية وأخلاقية وتقنية تتعلق بحمايتها وضمان استخدامها بصورة مشروعة وآمنة.

ويشكل فهم طبيعة البيانات وأنواعها وقيمتها الاقتصادية خطوة أساسية قبل الانتقال إلى دراسة الخصوصية الرقمية، التي ستتناولها الفصول اللاحقة بوصفها أحد أهم التحديات التي تواجه المجتمعات في عصر الذكاء الاصطناعي.

الفصل الثالث: الخصوصية الرقمية

مقدمة الفصل

أصبحت الخصوصية الرقمية واحدة من أكثر القضايا أهمية وإثارة للجدل في العصر الرقمي. فمع التوسع الهائل في استخدام الإنترنت والهواتف الذكية ومنصات التواصل الاجتماعي والخدمات السحابية والذكاء الاصطناعي، أصبحت كميات غير مسبوقة من البيانات الشخصية تُجمع وتُخزن وتُحلل يومياً. ولم تعد الخصوصية تقتصر على حماية الأسرار الشخصية، بل أصبحت حقاً أساسياً يرتبط بحرية الفرد وكرامته واستقلاليته وقدرته على التحكم في معلوماته.

وتزداد أهمية الخصوصية الرقمية في عصر الذكاء الاصطناعي التوليدي، حيث تعتمد الأنظمة الذكية على كميات ضخمة من البيانات لتطوير خدماتها وتحسين أدائها، مما يثير تساؤلات جوهرية حول حدود جمع البيانات واستخدامها والجهات التي يمكنها الوصول إليها.

يهدف هذا الفصل إلى توضيح مفهوم الخصوصية الرقمية وأبعادها المختلفة، واستعراض تطورها التاريخي، وتحليل أبرز التحديات التي تواجهها في البيئة الرقمية الحديثة.

التعريف اللغوي للخصوصية

ترتبط الخصوصية بمفهوم الانفراد والاستقلال والحق في الاحتفاظ ببعض الجوانب الشخصية بعيداً عن اطلاع الآخرين.

وتشير الخصوصية إلى قدرة الفرد على التحكم بالمعلومات المتعلقة به، وتحديد من يمكنه الوصول إليها وكيفية استخدامها.

التعريف القانوني للخصوصية

يُنظر إلى الخصوصية في القانون على أنها حق أساسي من حقوق الإنسان.

وقد نصت المادة (12) من الإعلان العالمي لحقوق الإنسان على أنه:

"لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته".

كما أكدت العديد من الاتفاقيات الدولية والتشريعات الوطنية على حق الأفراد في حماية بياناتهم الشخصية ومنع استخدامها بصورة غير مشروعة.

التعريف التقني للخصوصية

في المجال التقني، تشير الخصوصية إلى:

قدرة الأفراد على التحكم في جمع بياناتهم الشخصية ومعالجتها ومشاركتها واستخدامها.

ويتضمن ذلك: معرفة البيانات التي يتم جمعها ومعرفة الجهة التي تجمعها ومعرفة الغرض من استخدامها والقدرة على تعديلها أو حذفها والقدرة على الاعتراض على بعض أشكال المعالجة.

الخصوصية في المجتمعات التقليدية

في المجتمعات التقليدية كانت الخصوصية ترتبط أساساً بالمكان المادي وومن الأمثلة: حرمة المنزل وسرية المراسلات وحماية الحياة الأسرية.

وكانت القدرة على مراقبة الأفراد محدودة بسبب ضعف وسائل الاتصال والتكنولوجيا.

الخصوصية في عصر المعلومات

مع ظهور الحواسيب وقواعد البيانات الإلكترونية في النصف الثاني من القرن العشرين، بدأ مفهوم الخصوصية يتوسع ليشمل المعلومات الشخصية المخزنة رقمياً.

وأصبح القلق يتركز على: جمع البيانات وتخزينها وتبادلها بين المؤسسات.

الخصوصية في العصر الرقمي

أدى انتشار الإنترنت والهواتف الذكية إلى تحول جذري في طبيعة الخصوصية.

فأصبح المستخدم ينتج بيانات بصورة مستمرة من خلال: التصفح والبحث والشراء الإلكتروني واستخدام التطبيقات ووسائل التواصل الاجتماعي.

وبالتالي لم تعد الخصوصية مرتبطة فقط بما يختاره الفرد من معلومات، بل أيضاً بالبيانات التي تُجمع عنه تلقائياً.

خصوصية المعلومات

تشير إلى حماية البيانات الشخصية من الوصول غير المصرح به ووتشمل: الاسم والبريد الإلكتروني ورقم الهاتف والبيانات المالية والبيانات الصحية.

خصوصية الاتصالات

تتعلق بحماية وسائل الاتصال المختلفة.

مثل: البريد الإلكتروني والرسائل النصية والمكالمات الهاتفية والمحادثات الإلكترونية ويُعد اعتراض الاتصالات دون إذن قانوني انتهاكاً خطيراً للخصوصية.

الخصوصية الجسدية

تتعلق بحماية البيانات البيولوجية والبيومترية للفرد ومن أمثلتها: بصمة الإصبع وبصمة الوجه وبصمة العين والحمض النووي.

الخصوصية السلوكية

تشير إلى حماية المعلومات المتعلقة بسلوك الفرد وأنشطته.

مثل: المواقع التي يزورها والمنتجات التي يشتريها والأشخاص الذين يتواصل معهم واهتماماته وهواياته.

مفهوم الهوية الرقمية

الهوية الرقمية هي التمثيل الإلكتروني للفرد عبر الإنترنت وتشمل جميع البيانات التي يمكن من خلالها التعرف على الشخص أو تمييزه.

مكونات الهوية الرقمية

البيانات المباشرة

مثل: الاسم والصورة الشخصية والرقم الوطني.

البيانات غير المباشرة

مثل: عنوان IP وبيانات الموقع الجغرافي ومعرفات الأجهزة وملفات تعريف الارتباط (Cookies).

البصمة الرقمية

يقصد بالبصمة الرقمية الأثر الذي يتركه الفرد أثناء استخدامه للإنترنت.

وتنقسم إلى:

البصمة النشطة

المعلومات التي ينشرها المستخدم بنفسه ومثل: المنشورات والتعليقات والصور.

البصمة السلبية

المعلومات التي تُجمع تلقائياً ومثل: سجل التصفح وبيانات الموقع وسجل الاستخدام.

الاقتصاد القائم على البيانات

تعتمد العديد من الشركات الحديثة على جمع وتحليل البيانات الشخصية كمصدر رئيسي للإيرادات.

وتستخدم البيانات في: الإعلانات الموجهة وتحسين المنتجات وتحليل الأسواق وتطوير الذكاء الاصطناعي.

وسائل التواصل الاجتماعي

أدت وسائل التواصل الاجتماعي إلى إعادة تعريف مفهوم الخصوصية.

فالكثير من المستخدمين يشاركون معلومات شخصية بشكل طوعي، مما يزيد من احتمالية: إساءة الاستخدام وسرقة الهوية والهندسة الاجتماعية.

الهواتف الذكية

تجمع الهواتف الذكية كماً هائلاً من البيانات.

ومنها: الموقع الجغرافي وجهات الاتصال والصور وسجل المكالمات والتطبيقات المستخدمة ووتثير هذه البيانات مخاوف متزايدة بشأن الخصوصية.

الحوسبة السحابية

أتاحت الحوسبة السحابية إمكانيات كبيرة لتخزين البيانات ومعالجتها، لكنها في الوقت ذاته طرحت تحديات تتعلق بـ: مكان تخزين البيانات والجهات التي يمكنها الوصول إليها وعمليات النقل عبر الحدود.

الخصوصية والذكاء الاصطناعي

جمع البيانات على نطاق واسع

تعتمد أنظمة الذكاء الاصطناعي الحديثة على كميات ضخمة من البيانات.

وقد تشمل هذه البيانات: النصوص والصور والتسجيلات الصوتية والتفاعلات البشرية ووهذا يثير تساؤلات حول مدى مشروعية جمع هذه البيانات واستخدامها.

التنبؤ بالسلوك البشري

أصبحت الأنظمة الذكية قادرة على تحليل البيانات للتنبؤ بسلوك الأفراد.

مثل: التفضيلات الشرائية والاهتمامات السياسية والسلوك الاجتماعي ووقد يؤدي ذلك إلى مخاطر تتعلق بالتأثير على قرارات الأفراد أو توجيهها.

التوصيف الآلي(Profiling)

يقصد به استخدام البيانات لإنشاء ملفات تعريف رقمية للأفراد.

وقد تتضمن هذه الملفات: مستوى الدخل والحالة الصحية والاهتمامات والميول الاستهلاكية وتفرض العديد من القوانين قيوداً على هذه الممارسات.

المراقبة الذكية

أصبحت تقنيات الذكاء الاصطناعي تستخدم في: التعرف على الوجوه وتحليل الفيديو ومراقبة الأنشطة.

ورغم فوائدها الأمنية، فإنها تثير مخاوف كبيرة تتعلق بالخصوصية والحريات الفردية.

مبادئ حماية الخصوصية الرقمية

مبدأ الشفافية

يجب إعلام الأفراد بطريقة واضحة حول: البيانات التي يتم جمعها والغرض من جمعها ومدة الاحتفاظ بها.

مبدأ الموافقة

يجب الحصول على موافقة حرة وواضحة قبل جمع البيانات الشخصية أو معالجتها.

مبدأ تقليل البيانات

يجب جمع الحد الأدنى من البيانات اللازمة لتحقيق الغرض المطلوب.

مبدأ الأمن

يجب حماية البيانات من: الاختراق والتسريب والتعديل غير المصرح به.

مبدأ المساءلة

يجب أن تتحمل المؤسسات مسؤولية حماية البيانات وإثبات امتثالها للمتطلبات القانونية.

الخصوصية كحق أساسي في عصر الذكاء الاصطناعي

لم تعد الخصوصية مجرد مسألة تقنية أو قانونية، بل أصبحت عنصراً أساسياً في حماية حقوق الإنسان والحفاظ على الثقة الرقمية.

فكلما ازدادت قدرة الأنظمة الذكية على جمع البيانات وتحليلها، ازدادت الحاجة إلى بناء أطر قانونية وأخلاقية تضمن تحقيق التوازن بين الابتكار وحماية الأفراد.

إن نجاح الاقتصاد الرقمي والذكاء الاصطناعي في المستقبل يعتمد إلى حد كبير على قدرة المجتمعات والمؤسسات على بناء بيئة رقمية تحترم الخصوصية وتضمن الاستخدام المسؤول للبيانات.

خاتمة الفصل

تناول هذا الفصل مفهوم الخصوصية الرقمية وتطورها التاريخي وأبعادها المختلفة، كما استعرض أبرز التحديات التي تواجهها في البيئة الرقمية الحديثة، خصوصاً مع انتشار الذكاء الاصطناعي والتقنيات المعتمدة على البيانات. وقد تبين أن الخصوصية لم تعد قضية فردية فحسب، بل أصبحت قضية مجتمعية واقتصادية وقانونية تتطلب توازناً دقيقاً بين الاستفادة من التكنولوجيا وحماية الحقوق الأساسية للأفراد.

وفي الفصل القادم سيتم الانتقال إلى دراسة **البيانات الشخصية وأنواعها وتصنيفاتها القانونية والتقنية** باعتبارها الركيزة الأساسية التي تقوم عليها جميع منظومات الخصوصية وحماية البيانات.

الفصل الرابع: البيانات الشخصية

مقدمة الفصل

تمثل البيانات الشخصية محور جميع أنظمة الخصوصية وحماية البيانات الحديثة، إذ أصبحت معظم الأنشطة الرقمية تعتمد بصورة مباشرة أو غير مباشرة على جمع ومعالجة معلومات الأفراد. ومع توسع استخدام الإنترنت والهواتف الذكية والحوسبة السحابية والذكاء الاصطناعي، أصبحت البيانات الشخصية مورداً استراتيجياً تستخدمه الحكومات والمؤسسات التجارية ومزودو الخدمات الرقمية في اتخاذ القرارات وتطوير المنتجات وتحسين تجربة المستخدم.

وفي المقابل، أدى هذا التوسع إلى زيادة المخاطر المرتبطة بإساءة استخدام البيانات أو تسريبها أو معالجتها دون علم أصحابها أو موافقتهم، مما دفع العديد من الدول والمنظمات الدولية إلى تطوير تشريعات وأنظمة متخصصة لحماية البيانات الشخصية وتنظيم عمليات جمعها واستخدامها.

يهدف هذا الفصل إلى دراسة مفهوم البيانات الشخصية، وأنواعها، وخصائصها، وتصنيفاتها المختلفة، بالإضافة إلى استعراض الحقوق المرتبطة بها في البيئة الرقمية الحديثة.

تعريف البيانات الشخصية

أي معلومات تتعلق بشخص طبيعي محدد أو يمكن التعرف عليه بشكل مباشر أو غير مباشر.

ويشمل ذلك أي معلومة تسمح بتحديد هوية الفرد سواء بمفردها أو عند دمجها مع بيانات أخرى.

وتتبنى معظم التشريعات الحديثة هذا المفهوم، بما في ذلك: اللائحة العامة لحماية البيانات الأوروبية (GDPR) وقانون حماية البيانات الشخصية الأردني ونظام حماية البيانات الشخصية السعودي (PDPL) وقانون خصوصية المستهلك في كاليفورنيا (CCPA).

العناصر الأساسية للبيانات الشخصية

حتى تعتبر المعلومة بيانات شخصية يجب أن تحقق أحد الشرطين التاليين:

التحديد المباشر

عندما تسمح المعلومة بتحديد الشخص مباشرة ومثل: الاسم الكامل والرقم الوطني ورقم جواز السفر والصورة الشخصية.

التحديد غير المباشر

عندما يمكن استخدام المعلومة مع معلومات أخرى لتحديد هوية الشخص ومثل: عنوان IP والموقع الجغرافي ومعرف الجهاز والبريد الإلكتروني المهني.

البيانات التعريفية

وهي البيانات المستخدمة للتعرف على هوية الفرد.

أمثلة: الاسم وتاريخ الميلاد والجنس والجنسية والرقم الوطني وتعتبر من أكثر أنواع البيانات استخداماً في الأنظمة الحكومية والتجارية.

بيانات الاتصال

تستخدم للتواصل مع الفرد وتشمل: رقم الهاتف والبريد الإلكتروني وعنوان السكن وعنوان العمل.

البيانات المالية

تشمل المعلومات المرتبطة بالوضع المالي للفرد.

مثل: الحسابات البنكية والبطاقات الائتمانية والقروض والرواتب والمعاملات المالية وتتطلب مستويات عالية من الحماية نظراً لحساسيتها.

البيانات المهنية

ترتبط بالوضع الوظيفي أو المهني للفرد.

ومن أمثلتها: المسمى الوظيفي وجهة العمل والمؤهلات العلمية والسيرة الذاتية وسجلات الأداء الوظيفي.

البيانات التعليمية

تشمل المعلومات المرتبطة بالمسار التعليمي ومثل: الشهادات الأكاديمية والسجلات الدراسية والدرجات والتقارير التعليمية.

مفهوم البيانات الحساسة

تمثل البيانات الحساسة فئة خاصة من البيانات الشخصية تتطلب مستوى أعلى من الحماية القانونية والتنظيمية.

ويرجع ذلك إلى أن إساءة استخدامها قد تؤدي إلى: التمييز والابتزاز والإضرار بالسمعة والإضرار بالحقوق الأساسية للأفراد.

البيانات الصحية

تشمل: السجلات الطبية ونتائج الفحوصات والتشخيصات الطبية والوصفات العلاجية والتاريخ المرضي وتعد من أكثر أنواع البيانات حساسية في العالم.

البيانات البيومترية

البيانات البيومترية هي الخصائص البيولوجية أو السلوكية الفريدة التي يمكن استخدامها للتعرف على هوية الفرد.

مثل: بصمة الإصبع وبصمة الوجه وبصمة العين وبصمة الصوت وبصمة الكف.

البيانات الجينية

تشمل المعلومات المستخرجة من الحمض النووي.(DNA)

وتتميز بأنها: فريدة لكل فرد وثابتة نسبياً مدى الحياة وقد تكشف معلومات عن أفراد الأسرة أيضاً.

الآراء السياسية والمعتقدات الدينية

تحمي العديد من القوانين هذه البيانات بشكل خاص نظراً لإمكانية استخدامها في: التمييز والاستهداف السياسي والتضييق على الحريات الفردية.

السجل الجنائي

يتضمن: الأحكام القضائية والسوابق الجنائية والتحقيقات الجنائية وغالبا ما تفرض التشريعات قيوداً صارمة على معالجته.

البيانات العامة

هي البيانات التي يمكن نشرها أو مشاركتها دون أن يترتب على ذلك ضرر جوهري للفرد ومثل: الاسم الوظيفي والمؤهلات العامة والمعلومات المنشورة بإرادة صاحبها.

البيانات الداخلية

تستخدم داخل المؤسسة فقط ومثل: البريد الإلكتروني الداخلي وبيانات الموظفين التشغيلية والتقارير الإدارية.

البيانات السرية

تتطلب حماية إضافية ومثل: معلومات العملاء والبيانات المالية والعقود.

البيانات شديدة الحساسية

تمثل أعلى درجات التصنيف الأمني ومثل: البيانات الطبية والبيانات البيومترية والبيانات الأمنية وبيانات الأطفال.

دورة حياة البيانات الشخصية

جمع البيانات

مرحلة البداية في دورة حياة البيانات، وتُعالَج مصادرها وضوابطها القانونية بالتفصيل في الفصل السادس.

تخزين البيانات

يجب مراعاة: التشفير والتحكم بالصلاحيات والنسخ الاحتياطي وأمن البنية التحتية.

معالجة البيانات

تشمل: التحليل والتصنيف والنقل والمشاركة واستخدام الذكاء الاصطناعي.

الاحتفاظ بالبيانات

ينبغي ألا تحتفظ المؤسسات بالبيانات لفترة أطول من الحاجة الفعلية.

ويعرف هذا بمبدأ: تقييد فترة الاحتفاظ(Storage Limitation)

حذف البيانات

عند انتهاء الغرض من المعالجة يجب: حذف البيانات وإتلافها بشكل آمن وأو جعلها مجهولة الهوية.

حقوق أصحاب البيانات

الحق في المعرفة

يحق للفرد معرفة: ما البيانات التي يتم جمعها وسبب جمعها والجهة التي تعالجها.

حق الوصول

يحق للفرد الحصول على نسخة من بياناته الشخصية.

حق التصحيح

يحق للفرد طلب تصحيح البيانات غير الدقيقة أو غير المكتملة.

حق المحو

يعرف أحياناً باسم:

الحق في النسيان(Right to be Forgotten)

ويمنح الأفراد حق طلب حذف بياناتهم في ظروف محددة.

حق تقييد المعالجة

يمكن للفرد طلب الحد من استخدام بياناته في بعض الحالات.

حق الاعتراض

يحق للفرد الاعتراض على بعض أنواع المعالجة ومثل: التسويق المباشر والتوصيف الآلي وبعض القرارات المؤتمتة.

حق نقل البيانات

يمكن للفرد طلب نقل بياناته إلى مزود خدمة آخر بصيغة قابلة للقراءة الآلية.

البيانات الشخصية في عصر الذكاء الاصطناعي

البيانات كمصدر لتدريب النماذج

تعتمد أنظمة الذكاء الاصطناعي الحديثة على كميات ضخمة من البيانات ووقد تتضمن هذه البيانات: نصوصاً وصوراً وأصواتاً وسجلات رقمية.

وهذا يثير تحديات قانونية وأخلاقية تتعلق بمشروعية استخدام البيانات في التدريب.

مخاطر إعادة إنتاج البيانات

قد تظهر بعض النماذج سلوكيات تؤدي إلى إعادة إنتاج معلومات سبق أن تدربت عليها.

وتعرف هذه الظاهرة باسم: **Regurgitation**

وتشكل تحدياً مهماً في مجال حماية البيانات.

إخفاء الهوية وتخفيف المخاطر

من الوسائل المستخدمة للحد من المخاطر: إزالة المعرفات المباشرة والتعمية (Masking) والتشفير وإخفاء الهوية (Anonymization) واستخدام البيانات الاصطناعية.

أفضل الممارسات لحماية البيانات الشخصية

ينبغي على المؤسسات والأفراد الالتزام بمجموعة من الممارسات الأساسية: جمع الحد الأدنى من البيانات وتحديد أغراض المعالجة بوضوح وتطبيق ضوابط أمنية قوية وتدريب الموظفين على حماية البيانات ومراجعة الصلاحيات بشكل دوري وتطبيق مبدأ الخصوصية منذ التصميم (Design Privacy by) وتقييم المخاطر بشكل مستمر.

خاتمة الفصل

تُعد البيانات الشخصية حجر الأساس في منظومة الخصوصية الرقمية وحماية البيانات. وقد أدى التوسع في استخدام التكنولوجيا والذكاء الاصطناعي إلى زيادة أهمية هذه البيانات وتعقيد التحديات المرتبطة بها. كما أصبح من الضروري فهم أنواع البيانات الشخصية وتصنيفاتها المختلفة والحقوق القانونية المرتبطة بها لضمان استخدامها بصورة مسؤولة ومتوافقة مع التشريعات الحديثة.

وفي الفصل القادم سيتم تناول **مبادئ حماية البيانات الشخصية** التي تشكل الأساس القانوني والتنظيمي الذي تستند إليه معظم الأنظمة والتشريعات العالمية المعاصرة.

الفصل الخامس: مبادئ حماية البيانات الشخصية

مقدمة الفصل

تمثل مبادئ حماية البيانات الشخصية الأساس الذي تقوم عليه التشريعات والسياسات الحديثة المتعلقة بالخصوصية وإدارة المعلومات. وعلى الرغم من اختلاف الأنظمة القانونية بين الدول، فإن معظم قوانين حماية البيانات في العالم تستند إلى مجموعة مشتركة من المبادئ التي تهدف إلى ضمان الاستخدام العادل والمسؤول للبيانات الشخصية.

وقد تبنت هذه المبادئ العديد من الأطر التنظيمية الدولية، بما في ذلك اللائحة العامة لحماية البيانات الأوروبية(GDPR) ، وقانون حماية البيانات الشخصية الأردني، ونظام حماية البيانات الشخصية السعودي(PDPL) ، وغيرها من التشريعات الحديثة.

وتكمن أهمية هذه المبادئ في أنها توفر إطاراً عملياً للمؤسسات والأفراد لفهم كيفية جمع البيانات ومعالجتها واستخدامها بصورة قانونية وأخلاقية وآمنة.

مفهوم المشروعية

يقضي هذا المبدأ بأن تتم جميع عمليات معالجة البيانات الشخصية وفق أساس قانوني واضح ومشروع.

ويعني ذلك أن المؤسسة لا يجوز لها جمع أو استخدام البيانات الشخصية بشكل عشوائي أو دون مبرر قانوني.

ومن أمثلة الأسس القانونية المشروعة: موافقة صاحب البيانات وتنفيذ عقد والالتزام القانوني وحماية المصالح الحيوية والمصلحة العامة والمصلحة المشروعة للمؤسسة.

مفهوم العدالة

يشترط هذا المبدأ أن تتم معالجة البيانات بطريقة عادلة لا تؤدي إلى الإضرار بالأفراد أو التمييز ضدهم.

ومن صور المعالجة غير العادلة: جمع بيانات لا يحتاجها الغرض الأساسي واستخدام البيانات لأغراض مختلفة دون علم صاحبها واتخاذ قرارات مؤثرة بناءً على معلومات غير دقيقة.

مفهوم الشفافية

يقصد بالشفافية إبلاغ الأفراد بصورة واضحة ومفهومة حول: نوع البيانات التي يتم جمعها وسبب جمعها وكيفية استخدامها والجهات التي ستشارك معها ومدة الاحتفاظ بها وويجب أن تكون هذه المعلومات مكتوبة بلغة بسيطة ومفهومة.

مبدأ تحديد الغرض

مفهوم المبدأ

يعد تحديد الغرض أحد أهم مبادئ حماية البيانات.

وينص على أن البيانات يجب أن تجمع لأغراض: محددة وواضحة ومشروعة وولا يجوز استخدامها لاحقاً لأغراض أخرى غير متوافقة مع الغرض الأصلي.

أهمية تحديد الغرض

يساعد هذا المبدأ على: منع إساءة استخدام البيانات وتعزيز الثقة بين الأفراد والمؤسسات وتقليل المخاطر القانونية وتعزيز الامتثال التنظيمي.

أمثلة تطبيقية

إذا قامت جامعة بجمع بيانات الطلبة لأغراض التسجيل الأكاديمي، فلا يجوز استخدامها لأغراض تسويقية دون موافقة مستقلة.

وإذا جمعت مؤسسة صحية بيانات المرضى للعلاج، فلا يجوز مشاركتها مع جهات أخرى لأغراض تجارية.

مبدأ تقليل البيانات

مفهوم المبدأ

ينص هذا المبدأ على ضرورة جمع الحد الأدنى من البيانات اللازمة لتحقيق الغرض المطلوب.

ويعرف هذا المفهوم باسم: Data Minimization

أهمية المبدأ

كلما زادت كمية البيانات المخزنة زادت: احتمالية التسريب ومخاطر الاختراق وتكاليف الإدارة والحماية والمسؤوليات القانونية.

أمثلة عملية

إذا كان نموذج التسجيل يحتاج فقط إلى: الاسم والبريد الإلكتروني.

فلا ينبغي طلب: الرقم الوطني والحالة الصحية وبيانات أفراد الأسرة وما لم يكن هناك سبب مشروع لذلك.

مفهوم الدقة

يجب أن تكون البيانات الشخصية: صحيحة ودقيقة ومحدثة وبقدر الإمكان.

مخاطر البيانات غير الدقيقة

قد تؤدي البيانات الخاطئة إلى: قرارات غير عادلة ورفض خدمات بصورة خاطئة وأضرار مالية وأضرار قانونية.

مسؤولية المؤسسة

يتوجب على المؤسسات: مراجعة البيانات دورياً وتوفير آليات للتحديث وتمكين الأفراد من تصحيح بياناتهم.

مبدأ تقييد فترة الاحتفاظ

مفهوم المبدأ

ينص هذا المبدأ على عدم الاحتفاظ بالبيانات لفترة أطول من الحاجة الفعلية.

ويعرف أيضاً باسم Storage Limitation

أهمية المبدأ

كلما طال الاحتفاظ بالبيانات زادت: فرص الاختراق واحتمالات سوء الاستخدام والمسؤوليات القانونية.

سياسات الاحتفاظ

يجب أن تمتلك كل مؤسسة سياسة واضحة تحدد: مدة الاحتفاظ بكل نوع من البيانات وأسلوب الأرشفة وآلية الحذف الآمن.

مبدأ السلامة والسرية

مفهوم المبدأ

يقضي هذا المبدأ بحماية البيانات من: الوصول غير المصرح به والفقدان والتعديل والتدمير والتسريب.

الضوابط التقنية

تشمل: التشفير حماية البيانات أثناء التخزين والنقل والتحكم بالوصول منح الصلاحيات حسب الحاجة الفعلية والمصادقة متعددة العوامل تعزيز أمن الحسابات والنسخ الاحتياطي ضمان استمرارية الأعمال.

الضوابط الإدارية

تشمل: السياسات والإجراءات والتدريب والتوعية وتقييم المخاطر وإدارة الحوادث الأمنية.

مفهوم المساءلة

يعد مبدأ المساءلة من أهم المبادئ الحديثة في حماية البيانات.

ويعني أن المؤسسة لا تكتفي بالامتثال فقط، بل يجب أن تكون قادرة على إثبات امتثالها.

عناصر المساءلة

تشمل: توثيق العمليات والاحتفاظ بالسجلات وإجراء التدقيقات وتقييم المخاطر وإثبات الامتثال عند الطلب.

مسؤولية الإدارة العليا

لا تقع مسؤولية حماية البيانات على قسم تقنية المعلومات فقط، بل تشمل: الإدارة التنفيذية والإدارة القانونية والموارد البشرية وجميع الموظفين.

مفهومPrivacy by Design

يقضي هذا المبدأ بأن تؤخذ الخصوصية بعين الاعتبار منذ المراحل الأولى لتصميم الأنظمة والخدمات.

وليس بعد الانتهاء من تطويرها.

عناصر الخصوصية منذ التصميم

التوقع المسبق للمخاطر تحديد التهديدات المحتملة قبل وقوعها والحماية الافتراضية تفعيل أعلى مستويات الخصوصية بشكل افتراضي ودمج الخصوصية في التصميم اعتبار الخصوصية جزءاً من النظام نفسه.

أهمية المبدأ في الذكاء الاصطناعي

في الأنظمة الذكية الحديثة يجب مراعاة: تقليل البيانات المستخدمة للتدريب وإزالة المعرفات الشخصية ومنع كشف البيانات الحساسة وتعزيز الشفافية.

الخصوصية افتراضياً

مفهومPrivacy by Default

يعني أن تكون إعدادات الخصوصية الأكثر حماية مفعلة تلقائياً دون الحاجة إلى تدخل المستخدم.

تطبيقات عملية

عدم مشاركة البيانات تلقائياً وتعطيل التتبع غير الضروري وتقليل جمع البيانات وإخفاء المعلومات الحساسة بشكل افتراضي.

تحديات الذكاء الاصطناعي

تواجه تطبيقات الذكاء الاصطناعي تحديات خاصة مثل: ضخامة البيانات المستخدمة وصعوبة تفسير بعض النماذج واحتمالية التحيز وإعادة إنتاج البيانات التدريبية.

دور مبادئ حماية البيانات

تساعد هذه المبادئ على: ضبط استخدام البيانات وتقليل المخاطر القانونية وتعزيز الثقة وحماية حقوق الأفراد.

الامتثال في عصر الذكاء الاصطناعي

أصبح تطبيق مبادئ حماية البيانات شرطاً أساسياً لنجاح مشاريع الذكاء الاصطناعي واستدامتها، خصوصاً في القطاعات الحساسة مثل: الصحة والتعليم والخدمات المالية والحكومة الإلكترونية.

خاتمة الفصل

تشكل مبادئ حماية البيانات الشخصية الإطار الأساسي الذي تستند إليه جميع التشريعات الحديثة المتعلقة بالخصوصية. وتوفر هذه المبادئ مجموعة من القواعد التي تضمن جمع البيانات ومعالجتها واستخدامها بصورة قانونية وآمنة وأخلاقية. كما تزداد أهميتها مع انتشار تقنيات الذكاء الاصطناعي التي تعتمد على كميات ضخمة من البيانات وتفرض تحديات جديدة تتطلب مستويات أعلى من الحوكمة والامتثال.

وفي الفصل القادم سيتم تناول **إدارة دورة حياة البيانات الشخصية** بصورة أكثر تفصيلاً، ابتداءً من مرحلة جمع البيانات وصولاً إلى أرشفتها أو حذفها، مع بيان الضوابط التقنية والقانونية المرتبطة بكل مرحلة.

الفصل السادس: إدارة دورة حياة البيانات الشخصية

مقدمة الفصل

لا تقتصر حماية البيانات الشخصية على تأمين قواعد البيانات أو منع الاختراقات فقط، بل تمتد لتشمل جميع المراحل التي تمر بها البيانات منذ لحظة جمعها وحتى التخلص منها بشكل نهائي. ويُطلق على هذه المراحل مصطلح **دورة حياة البيانات الشخصية.(Personal Data Lifecycle)**

وتُعد إدارة دورة حياة البيانات من الركائز الأساسية في أنظمة حماية البيانات الحديثة، حيث تساعد المؤسسات على تحقيق الامتثال القانوني، وتقليل المخاطر الأمنية، وتحسين جودة البيانات، وتعزيز ثقة الأفراد والمؤسسات.

وفي عصر الذكاء الاصطناعي والحوسبة السحابية، أصبحت إدارة دورة حياة البيانات أكثر تعقيداً بسبب زيادة حجم البيانات، وتعدد أماكن تخزينها، وكثرة الجهات التي تتعامل معها.

يهدف هذا الفصل إلى دراسة المراحل المختلفة لدورة حياة البيانات الشخصية والضوابط القانونية والتقنية المرتبطة بكل مرحلة.

تعريف دورة حياة البيانات

مجموعة المراحل التي تمر بها البيانات منذ إنشائها أو جمعها وحتى حذفها أو إتلافها بصورة نهائية.

وتشمل عادة: جمع البيانات وتصنيف البيانات وتخزين البيانات واستخدام البيانات ومشاركة البيانات وأرشفة البيانات وحذف البيانات أو إتلافها.

أهمية إدارة دورة الحياة

تساعد إدارة دورة الحياة على: تعزيز الامتثال القانوني وتقليل المخاطر الأمنية وتحسين جودة البيانات وتقليل تكاليف التخزين وتعزيز الثقة بين المؤسسات والأفراد.

مفهوم جمع البيانات

تمثل عملية جمع البيانات نقطة البداية في دورة الحياة.

ويقصد بها :الحصول على البيانات الشخصية من الأفراد أو من مصادر أخرى بطريقة مشروعة.

مصادر جمع البيانات

المصادر المباشرة

عندما يقدم الفرد البيانات بنفسه ومثل: نماذج التسجيل وطلبات التوظيف والاشتراكات الإلكترونية.

المصادر غير المباشرة

عندما تُجمع البيانات من جهات أخرى ومثل: المؤسسات الحكومية والشركاء التجاريين وقواعد البيانات المشتركة.

المصادر الآلية

تشمل البيانات التي يتم جمعها تلقائياً.

مثل: ملفات تعريف الارتباط (Cookies) وبيانات الموقع الجغرافي وسجلات الاستخدام ومعرفات الأجهزة.

الضوابط القانونية لجمع البيانات

يجب أن يكون جمع البيانات: مشروعاً ومحدد الغرض وشفافاً ومتناسباً مع الحاجة وويجب تجنب جمع بيانات غير ضرورية أو لا تخدم الغرض الأساسي.

أهمية التصنيف

يعد تصنيف البيانات خطوة أساسية لتحديد مستوى الحماية المطلوب وفليس جميع البيانات تحتاج إلى نفس مستوى الضوابط الأمنية.

مستويات التصنيف

بيانات عامة يمكن مشاركتها دون مخاطر كبيرة وبيانات داخلية تستخدم داخل المؤسسة فقط وبيانات سرية تحتاج إلى ضوابط وصول إضافية وبيانات شديدة الحساسية تتطلب أعلى مستويات الحماية.

فوائد التصنيف

يساعد التصنيف على: تحديد الصلاحيات وتطبيق الضوابط المناسبة وتحسين إدارة المخاطر وتسهيل الامتثال القانوني.

تخزين البيانات

مفهوم التخزين

بعد جمع البيانات وتصنيفها يتم تخزينها في أنظمة مختلفة ومثل: قواعد البيانات والخوادم المحلية والحوسبة السحابية وأنظمة الأرشفة.

متطلبات التخزين الآمن

التشفير يجب تشفير البيانات أثناء التخزين والنسخ الاحتياطي إنشاء نسخ احتياطية دورية والتحكم بالوصول تحديد من يحق له الاطلاع على البيانات والمراقبة تسجيل ومتابعة الأنشطة المرتبطة بالبيانات.

مخاطر التخزين

تشمل: الاختراقات الإلكترونية وتسرب البيانات وفقدان البيانات وإساءة استخدام الصلاحيات.

استخدام البيانات

مفهوم المعالجة

تشمل المعالجة أي عملية تتم على البيانات ومثل: التحليل والتصنيف والتعديل والنقل والربط والحذف.

الاستخدام المشروع

يجب أن يقتصر استخدام البيانات على الأغراض التي جُمعت من أجلها وولا يجوز توسيع الاستخدام دون أساس قانوني مناسب.

الذكاء الاصطناعي ومعالجة البيانات

في بيئات الذكاء الاصطناعي قد تستخدم البيانات في: تدريب النماذج واختبار النماذج وتحسين الأداء والتنبؤ واتخاذ القرار ووهنا تظهر أهمية التحقق من الامتثال لمبادئ حماية البيانات.

مفهوم مشاركة البيانات

يقصد بها إتاحة البيانات لطرف آخر وسواء كان: مؤسسة حكومية وشركة خاصة ومزود خدمة سحابية وشريكاً تجارياً.

مخاطر المشاركة

تشمل: فقدان السيطرة على البيانات وإساءة الاستخدام والمعالجة غير المشروعة ونقل البيانات إلى دول ذات حماية ضعيفة.

الضوابط القانونية

وجود أساس قانوني للمشاركة وتوثيق عمليات النقل وتوقيع اتفاقيات معالجة البيانات وتقييم مخاطر الأطراف الخارجية.

مفهوم الأرشفة

الأرشفة هي الاحتفاظ بالبيانات لفترات طويلة لأغراض: قانونية وتنظيمية وتاريخية وبحثية.

متطلبات الأرشفة

يجب أن تكون البيانات المؤرشفة: محمية ومحدودة الوصول وموثقة وقابلة للاسترجاع عند الحاجة.

مخاطر الأرشفة

قد تؤدي الأرشفة غير المنظمة إلى: زيادة احتمالية التسريب وارتفاع التكاليف ومخالفة قوانين الاحتفاظ بالبيانات.

حذف البيانات وإتلافها

أهمية الحذف

عند انتهاء الغرض من البيانات يجب التخلص منها بطريقة آمنة ويمثل ذلك جزءاً أساسياً من الامتثال لمبدأ تقييد فترة الاحتفاظ.

أساليب الحذف

الحذف المنطقي إزالة إمكانية الوصول إلى البيانات والحذف الآمن الكتابة فوق البيانات عدة مرات والإتلاف الفيزيائي تدمير وسائط التخزين مادياً.

الحق في المحو

تعترف معظم التشريعات الحديثة بحق الأفراد في طلب حذف بياناتهم في ظروف معينة.

ويعرف هذا الحق باسم:

الحق في النسيان(Right to be Forgotten)

إدارة دورة الحياة في البيئات السحابية

تحديات الحوسبة السحابية

تواجه المؤسسات تحديات إضافية مثل: عدم معرفة الموقع الفعلي للبيانات ونقل البيانات عبر الحدود والاعتماد على مزودي الخدمات.

أفضل الممارسات

اختيار مزودين موثوقين ومراجعة العقود وتشفير البيانات ومراقبة عمليات النقل.

دورة حياة البيانات في أنظمة الذكاء الاصطناعي

البيانات التدريبية

تمثل الأساس الذي تعتمد عليه النماذج الذكية ويجب التأكد من: قانونية جمعها وجودتها وخلوها من الانتهاكات.

البيانات المستنتجة

قد تنتج الأنظمة الذكية بيانات جديدة من خلال التحليل والاستنتاج ويجب التعامل معها وفق نفس الضوابط المطبقة على البيانات الأصلية.

إدارة المخاطر

ينبغي مراقبة: التحيزات والتسريبات وإساءة الاستخدام وإعادة إنتاج البيانات التدريبية.

نموذج حوكمة دورة الحياة

توصي أفضل الممارسات المؤسسية بتعيين مسؤوليات واضحة تشمل:

المسؤولية	الدور
تحديد أغراض الاستخدام	مالك البيانات
مراقبة الامتثال	مسؤول حماية البيانات
تطبيق الضوابط الأمنية	قسم تقنية المعلومات
مراجعة الالتزامات القانونية	الإدارة القانونية
التحقق من الامتثال	التدقيق الداخلي

خاتمة الفصل

تشكل إدارة دورة حياة البيانات الشخصية أحد أهم عناصر الحوكمة الحديثة للبيانات. فالحماية الفعالة لا تبدأ عند حدوث اختراق أو تسريب، بل تبدأ منذ اللحظة الأولى لجمع البيانات وتستمر حتى حذفها أو إتلافها بصورة نهائية. كما أن تطبيق الضوابط المناسبة في كل مرحلة من مراحل دورة الحياة يساهم في تقليل المخاطر الأمنية والقانونية وتعزيز الثقة في الأنظمة الرقمية.

الفصل السابع: مخاطر البيانات الشخصية والتهديدات الأمنية في العصر الرقمي

مقدمة الفصل

أدى التحول الرقمي المتسارع إلى زيادة الاعتماد على البيانات الشخصية في مختلف القطاعات الاقتصادية والاجتماعية والحكومية. ومع تزايد قيمة البيانات، أصبحت هدفاً رئيسياً للهجمات الإلكترونية والجرائم الرقمية، حيث تسعى الجهات الخبيثة إلى الحصول عليها أو استغلالها لتحقيق مكاسب مالية أو سياسية أو استخباراتية.

وفي الوقت الذي توفر فيه التكنولوجيا الحديثة فرصاً هائلة لتحسين الخدمات وتطوير الأعمال، فإنها تخلق أيضاً بيئة معقدة من المخاطر التي قد تهدد خصوصية الأفراد وأمن المؤسسات. وقد ازدادت هذه المخاطر تعقيداً مع ظهور الذكاء الاصطناعي التوليدي، الذي أضاف أبعاداً جديدة للهجمات السيبرانية وأساليب الاحتيال الرقمي.

يهدف هذا الفصل إلى استعراض أبرز التهديدات والمخاطر المرتبطة بالبيانات الشخصية، وتحليل آثارها على الأفراد والمؤسسات، وبيان أفضل الممارسات للحد منها.

تعريف مخاطر البيانات

يقصد بمخاطر البيانات الشخصية:

أي حدث أو ظرف قد يؤدي إلى فقدان سرية البيانات الشخصية أو سلامتها أو توافرها أو استخدامها بطريقة غير مشروعة.

وتشمل هذه المخاطر: الاختراقات الإلكترونية وإساءة الاستخدام الداخلي والأخطاء البشرية والكوارث التقنية والاحتيال الرقمي.

عناصر الخطر

يتكون الخطر عادة من ثلاثة عناصر رئيسية: الأصل (Asset) البيانات أو المعلومات المطلوب حمايتها والتهديد (Threat) العامل الذي قد يسبب الضرر والثغرة (Vulnerability) نقطة الضعف التي تسمح بحدوث الهجوم.

أثر المخاطر

قد تؤدي حوادث البيانات إلى: خسائر مالية وأضرار قانونية وفقدان الثقة وتعطيل الأعمال والإضرار بالسمعة المؤسسية.

اختراقات البيانات(Data Breaches)

مفهوم اختراق البيانات

اختراق البيانات هو حادث أمني يؤدي إلى: الوصول غير المصرح به والكشف غير المشروع وفقدان البيانات وتعديل البيانات وسواء بشكل متعمد أو غير متعمد.

أسباب اختراق البيانات

تشمل :الهجمات **الإلكترونية**

مثل: البرمجيات الخبيثة وهجمات الفدية واستغلال الثغرات.

الأخطاء البشرية

مثل: إرسال البيانات إلى جهة خاطئة وضعف كلمات المرور وسوء إعداد الأنظمة.

التهديدات الداخلية

قد يكون مصدر الخطر: موظفاً حالياً وموظفاً سابقاً ومتعاقداً خارجياً.

آثار اختراق البيانات

قد تشمل: كشف معلومات حساسة وسرقة الهوية والاحتيال المالي والغرامات التنظيمية والدعاوى القضائية.

مفهوم الهندسة الاجتماعية

الهندسة الاجتماعية هي:

استخدام الخداع والتلاعب النفسي لدفع الأشخاص إلى الكشف عن معلومات حساسة أو تنفيذ إجراءات غير آمنة.

وتعد من أكثر أساليب الهجوم نجاحاً بسبب استهدافها للعنصر البشري.

أساليب الهندسة الاجتماعية

انتحال الهوية يقوم المهاجم بالتظاهر بأنه: موظف دعم فني ومدير وجهة حكومية واستغلال الثقة استغلال العلاقات الشخصية أو المهنية للحصول على المعلومات.

إثارة الخوف أو الاستعجال

مثل" سيتم إغلاق حسابك خلال ساعة".

أسباب نجاح الهندسة الاجتماعية

قلة الوعي الأمني والثقة الزائدة وضعف التدريب والرغبة في المساعدة.

التصيد الإلكتروني(Phishing)

مفهوم التصيد الإلكتروني

التصيد الإلكتروني هو:

محاولة احتيالية تهدف إلى سرقة المعلومات الحساسة عبر رسائل أو مواقع مزيفة.

أنواع التصيد

التصيد عبر البريد الإلكتروني الأكثر انتشاراً والتصيد عبر الرسائل النصية (Smishing) يستخدم الرسائل القصيرة والتصيد عبر المكالمات (Vishing) يستخدم المكالمات الهاتفية والتصيد الموجه (Spear Phishing) يستهدف شخصاً أو مؤسسة محددة.

مؤشرات التصيد

روابط مشبوهة وأخطاء لغوية وطلب معلومات حساسة ورسائل عاجلة وغير معتادة.

مفهوم سرقة الهوية

تحدث عندما يتم استخدام بيانات شخص آخر دون إذنه ومثل: الاسم والرقم الوطني والحسابات البنكية والحسابات الإلكترونية.

مصادر سرقة الهوية

اختراق قواعد البيانات والتصيد الإلكتروني ووسائل التواصل الاجتماعي والمستندات المسربة.

آثار سرقة الهوية

خسائر مالية وتشويه السمعة ومشكلات قانونية وصعوبة استعادة الحسابات.

تعريف البرمجيات الخبيثة

هي برامج مصممة لإلحاق الضرر بالأنظمة أو سرقة المعلومات.

أنواع البرمجيات الخبيثة

الفيروسات تنتشر بين الملفات والديدان (Worms) تنتشر ذاتياً عبر الشبكات وأحصنة طروادة (Trojans) تبدو برامج شرعية لكنها خبيثة وبرامج التجسس (Spyware) تراقب المستخدم سراً وبرامج الفدية (Ransomware) تشفّر البيانات وتطلب فدية مالية.

تأثيرها على البيانات

قد تؤدي إلى: سرقة البيانات وحذف البيانات وتعطيل الأنظمة وتشفير الملفات.

مفهوم التهديد الداخلي

يقصد به المخاطر الناتجة عن أشخاص لديهم صلاحيات مشروعة للوصول إلى البيانات.

أنواع التهديدات الداخلية

التهديد المتعمد موظف يستغل صلاحياته لأغراض شخصية والتهديد غير المتعمد موظف يرتكب خطأ دون قصد.

أسباب التهديد الداخلي

ضعف الرقابة والصلاحيات الزائدة ونقص التدريب والدوافع المالية.

مخاطر الذكاء الاصطناعي على البيانات الشخصية

جمع البيانات الضخم

تعتمد أنظمة الذكاء الاصطناعي على كميات هائلة من البيانات.

وقد يؤدي ذلك إلى: جمع مفرط للبيانات وصعوبة تحديد مصدر البيانات وتحديات الامتثال القانوني.

إعادة إنتاج البيانات(Regurgitation)

قد تقوم بعض النماذج بإظهار معلومات مشابهة لبيانات التدريب ووهذا يمثل خطراً خصوصاً عند استخدام بيانات شخصية أو حساسة أثناء التدريب.

التحيز الخوارزمي

إذا كانت البيانات المستخدمة منحازة فقد تنتج الأنظمة: قرارات غير عادلة وتمييزاً غير مقصود ونتائج مضللة.

التزييف العميق(Deepfakes)

يستخدم الذكاء الاصطناعي لإنشاء: صور مزيفة وفيديوهات مزيفة وتسجيلات صوتية مزيفة ووقد تستخدم هذه التقنيات في: الاحتيال والتشهير والتضليل الإعلامي.

مخاطر الحوسبة السحابية

فقدان السيطرة المباشرة

عند تخزين البيانات في السحابة تصبح المؤسسة معتمدة على مزود الخدمة.

نقل البيانات عبر الحدود

قد يتم تخزين البيانات في دول مختلفة ذات مستويات حماية متفاوتة.

سوء الإعداد

تشير العديد من الدراسات إلى أن سوء إعداد الخدمات السحابية يعد سبباً رئيسياً لتسرب البيانات.

تقييم مخاطر البيانات

مفهوم تقييم المخاطر

هو عملية منهجية لتحديد: الأصول والتهديدات والثغرات والتأثيرات المحتملة.

خطوات تقييم المخاطر

تحديد البيانات، ما البيانات التي نملكها؟**، تحديد التهديدات،** ما المخاطر المحتملة؟

تحليل الأثر

ما حجم الضرر المتوقع؟

تحديد الضوابط

كيف يمكن تخفيف المخاطر؟

مصفوفة المخاطر

مستوى الخطر	التأثير	الاحتمالية
منخفض	منخفض	منخفض
متوسط	منخفض	مرتفع
حرج	مرتفع	مرتفع
متوسط	مرتفع	منخفض

استراتيجيات الحد من المخاطر

التوعية والتدريب

يعد العنصر البشري خط الدفاع الأول ويجب تنفيذ برامج توعية دورية.

التحكم بالصلاحيات

تطبيق مبدأ: أقل قدر من الصلاحيات(Least Privilege)

التشفير

حماية البيانات أثناء: التخزين والنقل والنسخ الاحتياطي.

المراقبة المستمرة

مراقبة: الحسابات والأنظمة والأنشطة المشبوهة.

خطط الاستجابة للحوادث

يجب أن تمتلك المؤسسة: فريق استجابة وإجراءات واضحة وآليات للإبلاغ والتعافي.

خاتمة الفصل

تمثل مخاطر البيانات الشخصية أحد أكبر التحديات التي تواجه الأفراد والمؤسسات في العصر الرقمي. ومع تطور الهجمات الإلكترونية وظهور تقنيات الذكاء الاصطناعي التوليدي، أصبحت حماية البيانات مسؤولية استراتيجية تتطلب مزيجاً من الضوابط التقنية والتنظيمية والقانونية والبشرية. ولا يمكن تحقيق حماية فعالة دون فهم طبيعة التهديدات ومصادرها وآثارها المحتملة.

الفصل الثامن: الأمن السيبراني وحماية البيانات الشخصية

مقدمة الفصل

أصبح الأمن السيبراني في العصر الرقمي أحد الركائز الأساسية لحماية البيانات الشخصية وضمان استمرارية الأعمال والخدمات الرقمية. فمع التوسع الهائل في استخدام الإنترنت والحوسبة السحابية والهواتف الذكية والذكاء الاصطناعي، ازدادت التهديدات الإلكترونية التي تستهدف الأفراد والمؤسسات والحكومات على حد سواء.

وتشير التقارير الدولية إلى أن الجرائم الإلكترونية أصبحت من أسرع أنواع الجرائم نمواً في العالم، حيث تتسبب سنوياً بخسائر تقدر بمليارات الدولارات نتيجة اختراق الأنظمة وسرقة البيانات وتعطيل الخدمات. وفي ظل اعتماد المؤسسات الحديثة على البيانات كأصل استراتيجي، أصبح الأمن السيبراني ضرورة تنظيمية وقانونية واقتصادية وليس مجرد خيار تقني.

يهدف هذا الفصل إلى توضيح مفهوم الأمن السيبراني وعلاقته بحماية البيانات الشخصية، واستعراض المبادئ الأساسية والأطر العالمية والضوابط التقنية والتنظيمية المستخدمة لحماية المعلومات.

تعريف الأمن السيبراني

يعرف الأمن السيبراني (Cybersecurity) بأنه:

مجموعة السياسات والإجراءات والتقنيات والضوابط المستخدمة لحماية الأنظمة والشبكات والبرامج والبيانات من الهجمات الإلكترونية أو الوصول غير المصرح به أو التدمير أو التعديل أو الإفصاح غير المشروع.

ويشمل الأمن السيبراني حماية: الأجهزة والشبكات والتطبيقات وقواعد البيانات والخدمات السحابية والمستخدمين.

أهمية الأمن السيبراني

تتمثل أهمية الأمن السيبراني في: **حماية البيانات** منع سرقة المعلومات أو تسريبها.\ **ضمان استمرارية الأعمال** تقليل احتمالية توقف الأنظمة والخدمات.

الامتثال القانوني

الالتزام بمتطلبات قوانين حماية البيانات.

الحفاظ على السمعة

حماية ثقة العملاء والشركاء.

تقليل الخسائر المالية

الحد من تكاليف الحوادث الأمنية.

المبادئ الأساسية للأمن السيبراني

السرية(Confidentiality)

تعني ضمان عدم وصول المعلومات إلا للأشخاص المصرح لهم بذلك وأمثلة تطبيقية: التشفير والتحكم بالصلاحيات والمصادقة متعددة العوامل.

السلامة(Integrity)

تعني المحافظة على دقة المعلومات وصحتها ومنع تعديلها بطريقة غير مشروعة وأمثلة: التوقيع الرقمي وسجلات التدقيق وأنظمة التحقق من التغيير.

التوافر(Availability)

يقصد به ضمان توفر البيانات والخدمات عند الحاجة إليها وأمثلة: النسخ الاحتياطي ومراكز البيانات الاحتياطية وخطط التعافي من الكوارث.

مثلثCIA

تشكل السرية والسلامة والتوافر ما يعرف باسم:

مثلث الأمن السيبراني(CIA Triad)

وهو النموذج الأساسي الذي تبنى عليه معظم برامج الأمن السيبراني الحديثة.

الضوابط الأمنية التقنية

التشفير

مفهوم التشفير

التشفير هو عملية تحويل البيانات إلى صيغة غير مفهومة بحيث لا يمكن قراءتها إلا من قبل الأشخاص المصرح لهم.

أنواع التشفير

التشفير أثناء التخزين يحمي البيانات المخزنة على الأقراص وقواعد البيانات والتشفير أثناء النقل يحمي البيانات أثناء انتقالها عبر الشبكات.

أهمية التشفير

يساعد على: منع التجسس وتقليل آثار الاختراق والامتثال للمتطلبات القانونية.

إدارة الهوية والوصول

مفهوم إدارة الهوية

تهدف إلى التحقق من هوية المستخدمين والتحكم في صلاحياتهم.

المصادقة(Authentication)

الإجابة على سؤال: من أنت؟

ومن وسائلها: كلمة المرور والبصمة ورمز التحقق.

التفويض(Authorization)

الإجابة على سؤال: ماذا يحق لك أن تفعل؟

مبدأ أقل الصلاحيات

يقضي بمنح المستخدم الحد الأدنى من الصلاحيات اللازمة لأداء عمله.

الجدران النارية

الجدار الناري (Firewall) هو نظام يراقب حركة البيانات الواردة والصادرة ويمنع الاتصالات غير المصرح بها.

أنظمة كشف التسلل

تستخدم للكشف عن الأنشطة المشبوهة داخل الشبكات والأنظمة.

وتشمل:

- IDSكشف التسلل
- IPSمنع التسلل

مكافحة البرمجيات الخبيثة

تشمل: برامج مكافحة الفيروسات وأنظمة الحماية من الفدية وأدوات كشف البرمجيات الضارة.

إدارة المخاطر السيبرانية

مفهوم إدارة المخاطر

هي عملية مستمرة تهدف إلى: تحديد المخاطر وتقييمها ومعالجتها ومراقبتها.

خطوات إدارة المخاطر

تحديد الأصول

مثل: قواعد البيانات والأنظمة والأجهزة.

تحديد التهديدات

مثل: الاختراقات والتسريب والفدية.

تقييم الاحتمالية

ما مدى احتمال وقوع التهديد؟

تقييم الأثر

ما حجم الضرر المتوقع؟

معالجة المخاطر

يمكن التعامل مع المخاطر من خلال: التخفيف تطبيق ضوابط أمنية والنقل مثل التأمين السيبراني والقبول عندما تكون تكلفة المعالجة أعلى من الخطر والتجنب إلغاء النشاط المسبب للخطر.

الأمن السيبراني والموارد البشرية

العامل البشري

تشير الدراسات إلى أن نسبة كبيرة من الحوادث الأمنية ترتبط بأخطاء بشرية وومن الأمثلة: كلمات مرور ضعيفة وفتح مرفقات ضارة ومشاركة بيانات حساسة.

التوعية الأمنية

يجب أن تشمل البرامج التدريبية: التصيد الإلكتروني وإدارة كلمات المرور وحماية البيانات والعمل عن بعد.

الثقافة الأمنية

الثقافة الأمنية تعني أن تصبح الحماية مسؤولية مشتركة بين جميع العاملين في المؤسسة.

الاستجابة للحوادث الأمنية

مفهوم الحادث الأمني

هو أي حدث يؤدي إلى: اختراق الأنظمة وتسريب البيانات وتعطيل الخدمات.

مراحل الاستجابة

التحضير إعداد السياسات والخطط والاكتشاف تحديد الحادث وتحليله والاحتواء منع انتشار الضرر والمعالجة إزالة السبب الجذري والتعافي استعادة الأنظمة والخدمات والمراجعة استخلاص الدروس المستفادة.

التعافي من الكوارث واستمرارية الأعمال

استمرارية الأعمال

تشمل الإجراءات التي تضمن استمرار الخدمات الأساسية أثناء الأزمات.

التعافي من الكوارث

يركز على استعادة الأنظمة بعد الحوادث الكبرى.

عناصر الخطة

النسخ الاحتياطي ومواقع بديلة وفرق الطوارئ وإجراءات الاستعادة.

الأمن السيبراني في البيئة السحابية

التحديات السحابية

تشمل: تعدد المواقع الجغرافية ومشاركة الموارد والاعتماد على مزودي الخدمة.

نموذج المسؤولية المشتركة

في الحوسبة السحابية: المزود مسؤول عن البنية التحتية والشبكات والخوادم والعميل مسؤول عن البيانات والمستخدمين والصلاحيات وإعدادات الأمان.

الأمن السيبراني والذكاء الاصطناعي

الذكاء الاصطناعي كأداة دفاعية

يمكن استخدام الذكاء الاصطناعي في: كشف الهجمات وتحليل السجلات واكتشاف الأنماط المشبوهة والاستجابة الآلية.

الذكاء الاصطناعي كأداة هجومية

قد يستخدم المهاجمون الذكاء الاصطناعي في: التصيد المتقدم وإنشاء برمجيات خبيثة والتزييف العميق وأتمتة الهجمات.

التحديات الجديدة

من أبرزها: تسميم البيانات (Data Poisoning) وهجمات التلاعب بالنماذج وسرقة النماذج واستنتاج البيانات الحساسة.

المعايير والأطر العالمية

معيار ISO 27001

يعد المعيار الدولي الأبرز لنظم إدارة أمن المعلومات ويهدف إلى: إدارة المخاطر وحماية المعلومات وتحسين الضوابط الأمنية.

إطار NIST Cybersecurity Framework

طور بواسطة المعهد الوطني الأمريكي للمعايير والتقنية.

ويعتمد على خمس وظائف رئيسية:

1. التحديد (Identify)
2. الحماية (Protect)
3. الكشف (Detect)
4. الاستجابة (Respond)
5. التعافي (Recover)

معيار ISO 27701

امتداد لمعيار ISO 27001 ويركز على إدارة الخصوصية وحماية البيانات الشخصية.

أفضل الممارسات المؤسسية

ينبغي على المؤسسات: تطبيق التشفير وتفعيل المصادقة متعددة العوامل ومراجعة الصلاحيات دورياً وتدريب الموظفين وإجراء اختبارات اختراق دورية ومراقبة الأنظمة باستمرار وإعداد خطط استجابة للحوادث وتنفيذ تقييمات المخاطر بانتظام والالتزام بالتشريعات والمعايير ودمج الأمن السيبراني ضمن استراتيجية المؤسسة.

خاتمة الفصل

يمثل الأمن السيبراني خط الدفاع الأول لحماية البيانات الشخصية في العصر الرقمي. فمع تزايد الاعتماد على البيانات والأنظمة الذكية، أصبحت المؤسسات مطالبة بتطبيق ضوابط تقنية

وتنظيمية متقدمة تضمن سرية المعلومات وسلامتها وتوافرها. كما أن نجاح برامج حماية البيانات يعتمد بشكل كبير على التكامل بين الأمن السيبراني والحوكمة والامتثال والتوعية البشرية.

الفصل التاسع: الإطار القانوني لحماية البيانات الشخصية

مقدمة الفصل

لم تعد حماية البيانات الشخصية مسألة تقنية أو إدارية فحسب، بل أصبحت قضية قانونية ترتبط بحقوق الإنسان والحريات الأساسية والتنمية الاقتصادية والأمن الوطني. ومع التطور السريع للتكنولوجيا الرقمية وانتشار الإنترنت والذكاء الاصطناعي والحوسبة السحابية، أدركت الحكومات والهيئات الدولية الحاجة إلى وضع أطر قانونية تنظم جمع البيانات الشخصية ومعالجتها واستخدامها ونقلها.

وخلال العقود الأخيرة شهد العالم ظهور عدد كبير من القوانين والأنظمة التي تهدف إلى تحقيق التوازن بين الاستفادة من البيانات وحماية حقوق الأفراد. وقد أصبحت هذه التشريعات تشكل جزءاً أساسياً من بيئة الأعمال الرقمية، حيث تفرض التزامات قانونية على المؤسسات وتمنح الأفراد حقوقاً متزايدة فيما يتعلق ببياناتهم الشخصية.

يهدف هذا الفصل إلى استعراض الأسس القانونية لحماية البيانات الشخصية، وبيان المبادئ التي تقوم عليها التشريعات الحديثة، وتحليل الاتجاهات العالمية في تنظيم البيانات والخصوصية.

الأساس القانوني لحماية البيانات

حماية البيانات كحق من حقوق الإنسان

تستند معظم قوانين حماية البيانات إلى مبدأ أساسي يتمثل في أن الخصوصية حق من حقوق الإنسان.

وقد نص الإعلان العالمي لحقوق الإنسان لعام 1948 على:

"لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته".

كما أكدت العديد من الاتفاقيات الدولية على حماية الحياة الخاصة للأفراد وبياناتهم الشخصية.

تطور التشريعات المتعلقة بالخصوصية

مرت التشريعات المتعلقة بالخصوصية بعدة مراحل: المرحلة الأولى حماية المراسلات والحياة الخاصة التقليدية والمرحلة الثانية تنظيم قواعد البيانات الإلكترونية والمرحلة الثالثة حماية البيانات الشخصية في البيئة الرقمية والمرحلة الرابعة تنظيم الذكاء الاصطناعي والبيانات الضخمة.

أهداف قوانين حماية البيانات

تهدف هذه القوانين إلى: حماية حقوق الأفراد وتعزيز الثقة الرقمية وتنظيم معالجة البيانات ومكافحة إساءة الاستخدام ودعم الاقتصاد الرقمي وتعزيز الأمن السيبراني.

المفاهيم القانونية الأساسية

صاحب البيانات(Data Subject)

هو الشخص الطبيعي الذي تتعلق به البيانات الشخصية ووقد يكون: مواطناً ومقيماً وموظفاً وعميلاً ومريضاً وطالباً.

المتحكم بالبيانات(Data Controller)

هو الشخص أو المؤسسة التي تحدد: أسباب جمع البيانات وطرق معالجتها وأغراض استخدامها.

معالج البيانات(Data Processor)

هو الجهة التي تعالج البيانات نيابة عن المتحكم ومثل: مزودي الخدمات السحابية وشركات الاستضافة ومزودي أنظمة إدارة الموارد.

المعالجة(Processing)

يقصد بالمعالجة أي عملية تتم على البيانات وتشمل: الجمع والتسجيل والتخزين والتعديل والنقل والمشاركة والحذف.

الأساس القانوني لمعالجة البيانات

الموافقة

تعد الموافقة من أكثر الأسس القانونية استخداماً.

ويجب أن تكون: حرة وصريحة ومحددة ومستنيرة ولا يجوز افتراض الموافقة أو إخفاؤها ضمن نصوص معقدة.

تنفيذ عقد

يجوز معالجة البيانات عندما تكون ضرورية لتنفيذ عقد مع صاحب البيانات ومثل: فتح حساب مصرفي والاشتراك في خدمة إلكترونية وإتمام عملية شراء.

الالتزام القانوني

يجوز معالجة البيانات إذا كان القانون يفرض ذلك ومثل: الالتزامات الضريبية ومتطلبات مكافحة غسل الأموال ومتطلبات الجهات الرقابية.

المصلحة العامة

تستخدم عادة في: الخدمات الحكومية والصحة العامة والإحصاءات الرسمية.

المصلحة المشروعة

قد تعتمد بعض المؤسسات على المصلحة المشروعة إذا: كانت المعالجة ضرورية ولم تتعارض مع حقوق الأفراد وأمكن تبريرها بصورة معقولة.

حقوق أصحاب البيانات

الحق في المعرفة

يحق للفرد معرفة: البيانات التي تجمع عنه والغرض من استخدامها والجهات التي تحصل عليها.

حق الوصول

الحصول على نسخة من البيانات الشخصية.

حق التصحيح

تصحيح المعلومات غير الدقيقة.

حق المحو

طلب حذف البيانات في ظروف محددة.

ويعرف أيضاً باسم: الحق في النسيان

حق الاعتراض

الاعتراض على بعض أنواع المعالجة ومثل: التسويق المباشر والتوصيف الآلي.

حق نقل البيانات

نقل البيانات إلى مزود خدمة آخر.

الحق في عدم الخضوع للقرارات الآلية

خصوصاً عندما تكون القرارات ذات أثر قانوني أو مالي جوهري.

الالتزامات القانونية للمؤسسات

الالتزام بالشفافية

يجب على المؤسسة تقديم إشعارات خصوصية واضحة ومفهومة.

حماية البيانات

تطبيق تدابير تقنية وتنظيمية مناسبة.

توثيق المعالجة

الاحتفاظ بسجلات توضح: أنواع البيانات وأغراض المعالجة وفترات الاحتفاظ.

الإبلاغ عن الحوادث

في العديد من التشريعات يجب الإبلاغ عن اختراقات البيانات خلال مدد زمنية محددة.

تعيين مسؤول حماية البيانات

في بعض الحالات يجب تعيين: مسؤول حماية بيانات(Data Protection Officer - DPO)

لمتابعة الامتثال والإشراف على حماية البيانات.

نقل البيانات عبر الحدود

مفهوم النقل الدولي للبيانات

يحدث عندما تنتقل البيانات من دولة إلى أخرى وسواء عبر: الحوسبة السحابية والشركات متعددة الجنسيات ومزودي الخدمات الخارجيين.

التحديات القانونية

تختلف مستويات الحماية بين الدول.

وقد يؤدي ذلك إلى: ضعف الضمانات القانونية وصعوبة إنفاذ الحقوق وزيادة مخاطر إساءة الاستخدام.

الضمانات المطلوبة

تشمل: العقود النموذجية وقرارات كفاية الحماية والضمانات المؤسسية الملزمة.

الخصوصية في بيئة العمل

بيانات الموظفين

تشمل: الملفات الوظيفية والرواتب والتقييمات والسجلات التأديبية.

المراقبة في بيئة العمل

يجب تحقيق توازن بين: مصالح المؤسسة وحقوق الموظفين ولا يجوز استخدام وسائل المراقبة بصورة تعسفية أو غير متناسبة.

المسؤولية القانونية والعقوبات

المسؤولية المدنية

قد تلتزم المؤسسة بتعويض الأفراد عن الأضرار الناتجة عن انتهاكات البيانات.

المسؤولية الإدارية

تشمل: الإنذارات والقرارات التصحيحية والغرامات.

المسؤولية الجنائية

في بعض الحالات قد تترتب مسؤولية جنائية عند: البيع غير المشروع للبيانات والإفصاح غير القانوني وإساءة استخدام البيانات الحساسة.

الذكاء الاصطناعي والتحديات القانونية الجديدة

البيانات التدريبية

أصبحت مشروعية استخدام البيانات في تدريب النماذج الذكية موضوعاً رئيسياً للنقاش القانوني العالمي.

التوصيف الآلي

تثير أنظمة الذكاء الاصطناعي مخاوف تتعلق بـ: التمييز والتحيز واتخاذ القرارات دون تدخل بشري.

الشفافية وقابلية التفسير

أصبحت العديد من الجهات التنظيمية تطالب بتوفير تفسيرات واضحة للقرارات التي تتخذها الأنظمة الذكية.

المسؤولية عن أخطاء الذكاء الاصطناعي

من أبرز الأسئلة القانونية المعاصرة:

- من المسؤول عن القرار الخاطئ؟
- من يتحمل الضرر؟
- كيف يمكن إثبات المسؤولية؟

الاتجاهات المستقبلية للتشريعات

تشير الاتجاهات العالمية إلى التركيز على: تنظيم الذكاء الاصطناعي وحماية الأطفال رقمياً والحد من المراقبة الجماعية وتعزيز حقوق الأفراد وزيادة العقوبات على الانتهاكات وتوحيد المعايير الدولية.

خاتمة الفصل

تشكل التشريعات القانونية حجر الأساس في منظومة حماية البيانات الشخصية، إذ توفر إطاراً ينظم العلاقة بين الأفراد والمؤسسات ويحدد الحقوق والالتزامات والمسؤوليات المرتبطة بالبيانات. ومع استمرار التطور التقني، أصبحت هذه التشريعات أكثر أهمية من أي وقت مضى، خصوصاً في ظل الانتشار الواسع للذكاء الاصطناعي والحوسبة السحابية والاقتصاد الرقمي.

الفصل العاشر: اللائحة العامة لحماية البيانات الأوروبية(GDPR)

مقدمة الفصل

تُعد اللائحة العامة لحماية البيانات الأوروبية - (General Data Protection Regulation GDPR)واحدة من أهم التشريعات القانونية في مجال حماية البيانات الشخصية على مستوى العالم. فمنذ دخولها حيز التنفيذ في 25 أيار/مايو 2018، أصبحت معياراً عالمياً تسترشد به الحكومات والمؤسسات عند تطوير قوانين الخصوصية وحماية البيانات.

ولا تقتصر أهمية GDPR على دول الاتحاد الأوروبي فحسب، بل تمتد آثارها إلى المؤسسات في مختلف أنحاء العالم، إذ تنطبق أحكامها على أي جهة تقوم بمعالجة بيانات أفراد موجودين داخل الاتحاد الأوروبي، بغض النظر عن موقع المؤسسة الجغرافي.

وقد ساهمت هذه اللائحة في إعادة تشكيل مفهوم الخصوصية الرقمية من خلال منح الأفراد حقوقاً واسعة على بياناتهم الشخصية، وفرض التزامات صارمة على المؤسسات، وإقرار عقوبات مالية كبيرة بحق الجهات المخالفة.

يهدف هذا الفصل إلى دراسة اللائحة العامة لحماية البيانات الأوروبية من حيث نشأتها وأهدافها ومبادئها الأساسية وحقوق الأفراد والالتزامات المفروضة على المؤسسات.

نشأة اللائحة العامة لحماية البيانات

الخلفية التاريخية

قبل صدور GDPR كان الاتحاد الأوروبي يعتمد على توجيه حماية البيانات الصادر عام 1995.

إلا أن التطور السريع للتكنولوجيا الرقمية أدى إلى ظهور تحديات جديدة لم تكن موجودة آنذاك، مثل: شبكات التواصل الاجتماعي والهواتف الذكية والحوسبة السحابية والبيانات الضخمة والذكاء الاصطناعي ولذلك بدأ الاتحاد الأوروبي عملية تحديث شاملة لقواعد حماية البيانات.

صدور اللائحة

تم اعتماد اللائحة الأوروبية عام 2016.

ودخلت حيز التنفيذ الكامل في: **25مايو 2018**

وأصبحت ملزمة لجميع الدول الأعضاء في الاتحاد الأوروبي.

أهداف اللائحة

تهدف GDPR إلى: تعزيز حقوق الأفراد وتوحيد قوانين حماية البيانات داخل أوروبا وتعزيز الثقة في الاقتصاد الرقمي ودعم الابتكار مع حماية الخصوصية وتنظيم نقل البيانات عبر الحدود.

نطاق تطبيق اللائحة

النطاق الجغرافي

من أبرز خصائص GDPR أنها ذات نطاق عابر للحدود.

فهي تنطبق على: المؤسسات داخل الاتحاد الأوروبي والمؤسسات خارج الاتحاد الأوروبي إذا كانت تقدم خدمات أو منتجات لأفراد داخل أوروبا والمؤسسات التي تراقب سلوك الأفراد داخل الاتحاد الأوروبي.

النطاق الموضوعي

تنطبق اللائحة على: جمع البيانات وتخزين البيانات وتحليل البيانات ومشاركة البيانات وحذف البيانات ووأي عملية أخرى تندرج ضمن مفهوم "المعالجة".

الاستثناءات

لا تنطبق اللائحة في بعض الحالات مثل: الاستخدام الشخصي البحت وبعض الأنشطة الأمنية والسيادية للدول وبعض الأنشطة الصحفية والأكاديمية وفق شروط محددة.

المبادئ الأساسية فيGDPR

تعتمد اللائحة على سبعة مبادئ رئيسية تشكل أساس جميع عمليات معالجة البيانات.

المشروعية والعدالة والشفافية

يجب أن تكون المعالجة: قانونية وعادلة وواضحة للأفراد ويجب إبلاغ صاحب البيانات بجميع التفاصيل المتعلقة بمعالجة بياناته.

تحديد الغرض

يجب جمع البيانات لأغراض: محددة ومشروعة ومعلنة مسبقاً ولا يجوز استخدامها لاحقاً لأغراض غير متوافقة.

تقليل البيانات

يجب ألا تجمع المؤسسة سوى البيانات الضرورية فقط ويعد هذا المبدأ من أهم أدوات تقليل المخاطر.

الدقة

يجب أن تكون البيانات: صحيحة ومحدثة وخالية من الأخطاء الجوهرية.

تقييد الاحتفاظ

لا يجوز الاحتفاظ بالبيانات لفترة أطول من الحاجة الفعلية.

السلامة والسرية

يجب حماية البيانات من: الاختراق والتعديل غير المشروع والإفصاح غير المصرح به.

المساءلة

يجب أن تكون المؤسسة قادرة على إثبات امتثالها لأحكام اللائحة.

الأسس القانونية للمعالجة

تنص المادة السادسة من GDPR على ستة أسس قانونية للمعالجة.

الموافقة

يجب أن تكون: حرة وصريحة ومحددة وقابلة للسحب.

تنفيذ عقد

إذا كانت المعالجة ضرورية لتنفيذ عقد مع الفرد.

الالتزام القانوني

عندما يفرض القانون على المؤسسة جمع أو معالجة البيانات.

حماية المصالح الحيوية

مثل حالات الطوارئ الطبية.

المصلحة العامة

مثل الأنشطة الحكومية والخدمات العامة.

المصلحة المشروعة

شريطة ألا تتعارض مع حقوق الأفراد وحرياتهم.

حقوق أصحاب البيانات

منحت GDPR الأفراد مجموعة واسعة من الحقوق.

الحق في الحصول على المعلومات

يحق للفرد معرفة: ما البيانات التي تجمع عنه وسبب جمعها وكيفية استخدامها.

حق الوصول

الحصول على نسخة من البيانات الشخصية.

حق التصحيح

تصحيح البيانات غير الدقيقة.

حق المحو

المعروف باسم: الحق في النسيان(Right to be Forgotten)

ويتيح طلب حذف البيانات في ظروف معينة.

حق تقييد المعالجة

تقليل أو إيقاف استخدام البيانات مؤقتاً.

حق نقل البيانات

الحصول على البيانات بصيغة قابلة للقراءة الآلية ونقلها إلى جهة أخرى.

حق الاعتراض

الاعتراض على بعض أنواع المعالجة وخصوصاً: التسويق المباشر والتوصيف الآلي.

الحق في عدم الخضوع للقرارات الآلية

خاصة القرارات ذات التأثير القانوني أو المالي.

البيانات الحساسة في GDPR

تمنح اللائحة حماية خاصة لفئات معينة من البيانات.

وتشمل: الأصل العرقي والآراء السياسية والمعتقدات الدينية والعضوية النقابية والبيانات الجينية والبيانات البيومترية والبيانات الصحية والحياة الجنسية ولا يجوز معالجتها إلا ضمن شروط قانونية صارمة.

مسؤول حماية البيانات (DPO)

مفهومDPO

هو شخص مستقل داخل المؤسسة يتولى: مراقبة الامتثال وتقديم المشورة والتواصل مع الجهات الرقابية.

متى يكون التعيين إلزامياً؟

يكون تعيين DPO إلزامياً في حالات معينة مثل: الجهات الحكومية والمعالجة واسعة النطاق للبيانات الحساسة والمراقبة المنتظمة للأفراد.

الإبلاغ عن اختراقات البيانات

مفهوم اختراق البيانات

أي حادث يؤدي إلى: فقدان البيانات وكشف البيانات والوصول غير المصرح به.

الإبلاغ للجهة الرقابية

توجب اللائحة الإبلاغ خلال: **72ساعة**

من اكتشاف الحادث إذا كان يشكل خطراً على الأفراد.

إبلاغ أصحاب البيانات

إذا كان الخطر مرتفعاً، يجب إبلاغ الأفراد المتأثرين دون تأخير غير مبرر.

نقل البيانات خارج الاتحاد الأوروبي

تفرض GDPR قيوداً صارمة على نقل البيانات إلى دول خارج الاتحاد الأوروبي.

ولا يسمح بالنقل إلا عند توفر: مستوى حماية مناسب وضمانات قانونية كافية واستثناء قانوني معترف به.

العقوبات والغرامات

تُعرف GDPR بصرامتها في العقوبات.

وتنقسم المخالفات إلى فئتين رئيسيتين:

الفئة الأولى غرامة تصل إلى: **10ملايين يورو** أو **2%من الإيرادات العالمية السنوية** أيهما أكبر.

الفئة الثانية

غرامة تصل إلى: **20مليون يورو** أو **4%من الإيرادات العالمية السنوية** أيهما أكبر.

GDPR :والذكاء الاصطناعي

أصبحت GDPR أحد أهم الأطر القانونية المؤثرة في تطوير أنظمة الذكاء الاصطناعي.

خصوصاً فيما يتعلق بـ:

البيانات التدريبية

ضرورة التأكد من قانونية البيانات المستخدمة.

الشفافية

توضيح كيفية استخدام البيانات.

القرارات الآلية

ضمان وجود إشراف بشري عند الحاجة.

تقليل البيانات

منع جمع كميات مفرطة من المعلومات.

الثاني عشر: أثر GDPR على العالم

أثرت GDPR في العديد من التشريعات الدولية.

ومن الأمثلة: قانون حماية البيانات الأردني والنظام السعودي لحماية البيانات الشخصية وقانون البرازيل LGPD وقوانين الخصوصية في العديد من الولايات الأمريكية وأصبحت معياراً عالمياً لحماية البيانات والخصوصية.

خاتمة الفصل

تمثل اللائحة العامة لحماية البيانات الأوروبية (GDPR) حجر الزاوية في منظومة حماية البيانات الحديثة، وقد ساهمت في إرساء مبادئ عالمية تتعلق بالشفافية والمساءلة وحقوق الأفراد. كما فرضت التزامات صارمة على المؤسسات وأعادت صياغة العلاقة بين الأفراد والجهات التي تجمع بياناتهم وتعالجها.

ومع استمرار تطور الذكاء الاصطناعي والاقتصاد الرقمي، ستبقى GDPR واحدة من أهم المرجعيات القانونية التي يستند إليها المشرعون والمؤسسات عند بناء سياسات الخصوصية وحماية البيانات.

الفصل القادم:

الفصل الحادي عشر: قانون حماية البيانات الشخصية الأردني رقم (24) لسنة 2023

- خلفية إصدار القانون
- التعاريف الأساسية
- حقوق أصحاب البيانات
- التزامات المتحكمين والمعالجين
- نقل البيانات خارج المملكة
- العقوبات والمسؤوليات القانونية
- أثر القانون على المؤسسات الأردنية والذكاء الاصطناعي.

الفصل الحادي عشر: قانون حماية البيانات الشخصية الأردني رقم (24) لسنة 2023

مقدمة الفصل

شهدت المملكة الأردنية الهاشمية خلال السنوات الأخيرة توسعاً ملحوظاً في استخدام التكنولوجيا الرقمية والخدمات الإلكترونية والذكاء الاصطناعي والحوسبة السحابية، الأمر الذي أدى إلى زيادة حجم البيانات الشخصية المتداولة بين المؤسسات الحكومية والخاصة. ومع هذا التحول الرقمي المتسارع، برزت الحاجة إلى إطار قانوني شامل ينظم عمليات جمع البيانات الشخصية ومعالجتها واستخدامها ويحمي حقوق الأفراد في مواجهة المخاطر المتزايدة المرتبطة بالخصوصية الرقمية.

وفي هذا السياق صدر **قانون حماية البيانات الشخصية الأردني رقم (24) لسنة 2023** ليشكل أول تشريع أردني متكامل يعالج موضوع حماية البيانات الشخصية بصورة شاملة. ويهدف القانون إلى تحقيق التوازن بين حماية خصوصية الأفراد من جهة، ودعم التحول الرقمي والابتكار والاستثمار من جهة أخرى.

ويمثل هذا القانون خطوة مهمة نحو مواءمة التشريعات الأردنية مع الاتجاهات الدولية الحديثة في مجال حماية البيانات والخصوصية.

خلفية إصدار القانون

التحول الرقمي في الأردن

شهد الأردن خلال العقدين الماضيين توسعاً كبيراً في: الخدمات الحكومية الإلكترونية والتجارة الإلكترونية والخدمات المصرفية الرقمية وتطبيقات الهواتف الذكية والحوسبة السحابية والذكاء الاصطناعي.

وقد أدى ذلك إلى زيادة حجم البيانات الشخصية التي يتم جمعها ومعالجتها يومياً.

الحاجة إلى التشريع

قبل صدور القانون كانت أحكام حماية البيانات موزعة بين عدة قوانين مختلفة مثل: قانون الجرائم الإلكترونية وقانون المعاملات الإلكترونية وقانون الاتصالات والتشريعات الجزائية والمدنية وإلا أنه لم يكن هناك قانون متخصص ينظم حماية البيانات الشخصية بشكل شامل.

أهداف القانون

يسعى القانون إلى تحقيق عدة أهداف رئيسية:

حماية الحقوق والحريات

ضمان حماية خصوصية الأفراد وبياناتهم الشخصية.

تعزيز الثقة الرقمية

تشجيع الأفراد على استخدام الخدمات الإلكترونية.

دعم الاقتصاد الرقمي

توفير بيئة قانونية مناسبة للاستثمار الرقمي.

تعزيز الامتثال الدولي

مواءمة التشريعات الأردنية مع المعايير العالمية.

نطاق تطبيق القانون

2.1الأشخاص المشمولون بالقانون

ينطبق القانون على: الأشخاص الطبيعيين والمؤسسات الخاصة والجهات الحكومية والمنظمات غير الربحية.

- الشركات الأجنبية التي تعالج بيانات داخل الأردن وفقاً للحالات التي يحددها القانون .

البيانات المشمولة

يشمل القانون جميع البيانات الشخصية التي تسمح بالتعرف على الشخص بصورة مباشرة أو غير مباشرة.

مثل: الاسم والرقم الوطني ورقم الهاتف والبريد الإلكتروني والموقع الجغرافي والبيانات البيومترية.

الاستثناءات

لا تسري بعض أحكام القانون على حالات محددة ينظمها القانون بصورة خاصة، مثل بعض الأنشطة الأمنية والقضائية وفق الضوابط القانونية المقررة.

التعريفات الأساسية في القانون

البيانات الشخصية

يعرف القانون البيانات الشخصية بأنها:

أي بيانات تتعلق بشخص طبيعي محدد الهوية أو قابل للتحديد بصورة مباشرة أو غير مباشرة.

البيانات الشخصية الحساسة

تشمل البيانات التي قد يؤدي كشفها أو إساءة استخدامها إلى إلحاق ضرر أكبر بصاحبها.

ومن أمثلتها: البيانات الصحية والبيانات البيومترية والبيانات الجينية والآراء السياسية والمعتقدات الدينية والسجل الجنائي.

صاحب البيانات

هو الشخص الطبيعي الذي تتعلق به البيانات الشخصية.

المتحكم بالبيانات

الشخص أو الجهة التي تحدد: غرض المعالجة ووسائل المعالجة وطريقة استخدام البيانات.

معالج البيانات

الشخص أو الجهة التي تقوم بمعالجة البيانات نيابة عن المتحكم.

مبادئ معالجة البيانات الشخصية

استند القانون إلى مجموعة من المبادئ الأساسية التي تشكل الأساس القانوني لمعالجة البيانات.

المشروعية

يجب أن تتم المعالجة وفق أساس قانوني مشروع.

الشفافية

يجب إعلام صاحب البيانات بكيفية استخدام بياناته.

تحديد الغرض

يجب جمع البيانات لغرض محدد ومشروع.

تقليل البيانات

جمع الحد الأدنى اللازم لتحقيق الغرض.

الدقة

يجب أن تكون البيانات صحيحة ومحدثة.

السرية والأمن

يجب توفير تدابير أمنية مناسبة لحماية البيانات.

حقوق أصحاب البيانات

يمنح القانون مجموعة من الحقوق الأساسية للأفراد.

الحق في العلم

يحق لصاحب البيانات معرفة: نوع البيانات التي يتم جمعها والغرض من المعالجة والجهات التي تحصل عليها.

حق الوصول

الحصول على نسخة من البيانات الشخصية.

حق التصحيح

تصحيح البيانات غير الدقيقة أو غير المكتملة.

حق سحب الموافقة

يجوز لصاحب البيانات سحب موافقته في أي وقت إذا كانت المعالجة تستند إلى الموافقة.

حق المحو أو الإخفاء

طلب حذف البيانات أو إخفاء الهوية في الحالات التي يسمح بها القانون.

حق تقييد المعالجة

طلب الحد من استخدام البيانات في ظروف معينة.

حق الاعتراض

الاعتراض على بعض أنواع المعالجة التي تمس حقوق الفرد أو مصالحه المشروعة.

التزامات المتحكمين والمعالجين

حماية البيانات

يلتزم المتحكم والمعالج باتخاذ تدابير تقنية وتنظيمية مناسبة لحماية البيانات.

توثيق العمليات

يجب الاحتفاظ بسجلات توضح: أنواع البيانات وأغراض المعالجة وفترات الاحتفاظ.

الإبلاغ عن الاختراقات

يلتزم المسؤولون بإبلاغ الجهات المختصة وأصحاب البيانات في بعض حالات اختراق البيانات وفق المدد المحددة قانوناً.

الحفاظ على السرية

يجب منع الوصول غير المصرح به إلى البيانات.

مجلس حماية البيانات الشخصية

إنشاء المجلس

أنشأ القانون مجلساً لحماية البيانات الشخصية يتولى الإشراف على تطبيق أحكام القانون.

مهام المجلس

تشمل: وضع السياسات العامة وإصدار التعليمات ومراقبة الامتثال والنظر في الشكاوى.

وحدة حماية البيانات

أنشأ القانون وحدة متخصصة لمتابعة تنفيذ أحكامه والتحقيق في المخالفات.

نقل البيانات خارج المملكة

مفهوم النقل الدولي

يقصد به نقل البيانات الشخصية إلى دولة أخرى أو إتاحتها لجهات خارج الأردن.

شروط النقل

يشترط القانون توفر مستوى مناسب من الحماية أو ضمانات قانونية تكفل حماية البيانات.

الاستثناءات

يجوز النقل في بعض الحالات الاستثنائية مثل: موافقة صاحب البيانات وتنفيذ عقد والضرورات القانونية والمصالح الحيوية.

البيانات الحساسة

يفرض القانون قيوداً إضافية على معالجة البيانات الحساسة.

ومن أمثلتها: البيانات الصحية والبيانات البيومترية والبيانات الجينية والبيانات المتعلقة بالأطفال وولا يجوز معالجتها إلا ضمن شروط قانونية محددة.

العقوبات والمسؤولية القانونية

العقوبات الإدارية

قد تشمل: الإنذارات وأوامر التصحيح ووقف المعالجة.

الغرامات المالية

يفرض القانون غرامات مالية على المخالفات وفق طبيعة المخالفة وجسامتها.

المسؤولية المدنية

يجوز للمتضررين المطالبة بالتعويض عن الأضرار الناتجة عن المخالفات.

المسؤولية الجزائية

قد تنشأ مسؤولية جنائية في بعض الحالات المتعلقة بإساءة استخدام البيانات أو الإفصاح غير المشروع عنها.

الحادي عشر: أثر القانون على المؤسسات الأردنية

القطاع الحكومي

يتطلب القانون مراجعة: قواعد البيانات الحكومية وسياسات الخصوصية وآليات تبادل البيانات.

القطاع المصرفي

يستلزم تعزيز: ضوابط الامتثال وحماية بيانات العملاء وإدارة المخاطر.

القطاع الصحي

يفرض متطلبات إضافية لحماية السجلات الطبية والبيانات الصحية.

القطاع التعليمي

يتطلب حماية بيانات الطلبة وأعضاء هيئة التدريس والباحثين.

قانون حماية البيانات والذكاء الاصطناعي

مع تزايد استخدام الذكاء الاصطناعي في الأردن، أصبح القانون مؤثراً بشكل مباشر على: تدريب النماذج الذكية ومعالجة البيانات الضخمة والتحليلات التنبؤية والأنظمة المؤتمتة.

ويجب على المؤسسات التأكد من أن استخدام البيانات في مشاريع الذكاء الاصطناعي يتم بصورة متوافقة مع أحكام القانون.

مقارنة بين القانون الأردني وGDPR

العنصر	القانون الأردني	GDPR

العنصر	القانون الأردني	GDPR
حماية البيانات الشخصية	نعم	نعم
حقوق الوصول والتصحيح	نعم	نعم
حق المحو	نعم	نعم
نقل البيانات عبر الحدود	منظم	منظم
مسؤول حماية البيانات	في حالات محددة	في حالات محددة
العقوبات المالية	موجودة	مرتفعة جداً
التأثير خارج الحدود	محدود	عالمي

خاتمة الفصل

يمثل قانون حماية البيانات الشخصية الأردني رقم (24) لسنة 2023 خطوة تشريعية مهمة في مسيرة التحول الرقمي الأردني، إذ يوفر إطاراً قانونياً متكاملاً لحماية البيانات الشخصية وتنظيم معالجتها. كما ينسجم في العديد من مبادئه مع أفضل الممارسات الدولية، ويعزز ثقة الأفراد والمؤسسات في البيئة الرقمية.

وتزداد أهمية هذا القانون مع التوسع في استخدام الذكاء الاصطناعي والحوسبة السحابية والبيانات الضخمة، حيث يشكل أساساً قانونياً لضمان الاستخدام المسؤول للبيانات الشخصية في الأردن.

الفصل القادم:

الفصل الثاني عشر: نظام حماية البيانات الشخصية السعودي (PDPL) والتشريعات العربية المقارنة

- نشأة النظام السعودي
- المبادئ الأساسية
- حقوق أصحاب البيانات

- التزامات الجهات المعالجة
- العقوبات
- مقارنة بين PDPL والقانون الأردني و GDPR
- مستقبل حماية البيانات في العالم العربي.

الفصل الثاني عشر: نظام حماية البيانات الشخصية السعودي **(PDPL)** والتشريعات العربية المقارنة

مقدمة الفصل

أصبحت حماية البيانات الشخصية أحد المحاور الرئيسية في استراتيجيات التحول الرقمي والتنمية الاقتصادية في الدول العربية. ومع ازدياد الاعتماد على الخدمات الإلكترونية والتجارة الرقمية والذكاء الاصطناعي والحوسبة السحابية، برزت الحاجة إلى تطوير أطر قانونية تنظم جمع البيانات الشخصية ومعالجتها واستخدامها بما يحقق التوازن بين الابتكار وحماية الحقوق الفردية.

وتُعد المملكة العربية السعودية من أوائل الدول العربية التي تبنت تشريعاً متكاملاً لحماية البيانات الشخصية من خلال **نظام حماية البيانات الشخصية - Personal Data Protection Law) (PDPL**، والذي يمثل خطوة مهمة نحو بناء بيئة رقمية آمنة ومتوافقة مع المعايير الدولية.

يهدف هذا الفصل إلى دراسة النظام السعودي لحماية البيانات الشخصية وتحليل أحكامه الرئيسية، مع إجراء مقارنة بينه وبين القانون الأردني واللائحة الأوروبيةGDPR ، واستعراض الاتجاهات المستقبلية لحماية البيانات في العالم العربي.

نشأة نظام حماية البيانات الشخصية السعودي

الخلفية التشريعية

جاء نظام حماية البيانات الشخصية السعودي ضمن رؤية المملكة العربية السعودية 2030 التي تهدف إلى: تعزيز الاقتصاد الرقمي وتطوير الحكومة الرقمية وجذب الاستثمارات التقنية وتعزيز الثقة في الخدمات الإلكترونية.

وقد أدى النمو السريع للخدمات الرقمية إلى الحاجة إلى تنظيم معالجة البيانات الشخصية بصورة أكثر وضوحاً.

إصدار النظام

صدر النظام لأول مرة عام 2021.

ثم أُدخلت عليه تعديلات مهمة خلال عام 2023 بهدف: تعزيز المرونة التنظيمية ومواءمة النظام مع المعايير الدولية ودعم الابتكار الرقمي وتسهيل الامتثال للمؤسسات.

الجهات المشرفة

تتولى الجهات المختصة في المملكة الإشراف على تطبيق النظام ومتابعة الامتثال والتحقيق في المخالفات وإصدار الأدلة التنظيمية ذات الصلة.

أهداف النظام السعودي

يسعى النظام إلى تحقيق مجموعة من الأهداف الرئيسية:

حماية خصوصية الأفراد

ضمان حماية البيانات الشخصية من الاستخدام غير المشروع.

تعزيز الثقة الرقمية

تشجيع الأفراد على استخدام الخدمات الرقمية بأمان.

دعم الاقتصاد الرقمي

تهيئة بيئة قانونية مناسبة للابتكار والاستثمار.

تنظيم المعالجة

وضع قواعد واضحة لجمع البيانات ومعالجتها وتخزينها ونقلها.

تعزيز الأمن السيبراني

رفع مستوى الحماية التقنية والتنظيمية للبيانات الشخصية.

المفاهيم الأساسية في النظام

البيانات الشخصية

يقصد بالبيانات الشخصية:

كل بيان يؤدي إلى معرفة الفرد على وجه التحديد أو يجعل التعرف عليه ممكناً بصورة مباشرة أو غير مباشرة.

البيانات الحساسة

تشمل البيانات التي قد يؤدي كشفها إلى مخاطر أكبر على الفرد.

مثل: البيانات الصحية والبيانات الوراثية والبيانات البيومترية والمعتقدات الدينية والخلفيات العرقية.

صاحب البيانات

هو الشخص الطبيعي الذي تتعلق به البيانات.

الجهة المتحكمة

هي الجهة التي تحدد: الغرض من جمع البيانات وطريقة معالجتها ووسائل استخدامها.

الجهة المعالجة

هي الجهة التي تعالج البيانات نيابة عن المتحكم.

المبادئ الأساسية للنظام

المشروعية

يجب أن تستند المعالجة إلى أساس قانوني مشروع.

الشفافية

يجب إبلاغ صاحب البيانات بوضوح حول كيفية استخدام بياناته.

تحديد الغرض

جمع البيانات لأغراض محددة ومعلنة.

تقليل البيانات

جمع الحد الأدنى اللازم لتحقيق الغرض.

الأمن والحماية

توفير الضوابط التقنية والتنظيمية المناسبة لحماية البيانات.

الدقة

الحفاظ على صحة البيانات وتحديثها عند الحاجة.

حقوق أصحاب البيانات

يمنح النظام السعودي أصحاب البيانات مجموعة من الحقوق المهمة.

الحق في العلم

معرفة: الغرض من جمع البيانات وطريقة معالجتها والجهات التي ستصل إليها.

حق الوصول

الحصول على نسخة من البيانات الشخصية.

حق التصحيح

تعديل البيانات غير الدقيقة أو غير المكتملة.

حق الإتلاف

طلب إتلاف البيانات عند انتهاء الغرض منها وفق الضوابط القانونية.

حق سحب الموافقة

إلغاء الموافقة الممنوحة لمعالجة البيانات متى كان ذلك ممكناً قانوناً.

التزامات الجهات المتحكمة والمعالجة

حماية البيانات

تطبيق ضوابط تقنية وتنظيمية مناسبة.

توثيق المعالجة

الاحتفاظ بسجلات واضحة لعمليات المعالجة.

الإبلاغ عن الحوادث

الإبلاغ عن حوادث اختراق البيانات عند تحقق شروط معينة.

تعيين مسؤول مختص

في بعض الحالات يجب تعيين مسؤول أو جهة مختصة بمتابعة الامتثال.

تقييم المخاطر

إجراء تقييمات دورية للمخاطر المرتبطة بمعالجة البيانات.

نقل البيانات خارج المملكة

مفهوم النقل الدولي

يقصد به نقل البيانات الشخصية إلى دولة أخرى أو إتاحتها لجهة خارج المملكة.

شروط النقل

يخضع النقل لشروط وضمانات محددة تهدف إلى حماية البيانات ومنع إساءة استخدامها.

الضمانات المطلوبة

تشمل: حماية كافية للبيانات وأغراض مشروعة للنقل والتزامات تعاقدية مناسبة.

العقوبات والمسؤوليات

الغرامات المالية

يفرض النظام عقوبات مالية على المخالفات وفق طبيعتها وخطورتها.

العقوبات الجنائية

في بعض الحالات الخطيرة قد تترتب مسؤوليات جزائية.

المسؤولية المدنية

يجوز المطالبة بالتعويض عن الأضرار الناتجة عن المخالفات.

مقارنة بين النظام السعودي و GDPRوالقانون الأردني

أوجه التشابه

تشترك الأنظمة الثلاثة في: حماية البيانات الشخصية وتنظيم المعالجة ومنح حقوق للأفراد وفرض التزامات على المؤسسات وتنظيم نقل البيانات عبر الحدود.

أوجه الاختلاف

العنصر	GDPR	القانون الأردني	PDPLالسعودي
النطاق الدولي	واسع جداً	محدود نسبياً	متوسط
حق نقل البيانات	متقدم	موجود	موجود
حق المحو	متقدم	موجود	موجود
العقوبات	مرتفعة جداً	متوسطة	مرتفعة
الإطار التنظيمي	ناضج جداً	حديث	حديث ومتطور
التطبيق خارج الحدود	واضح	محدود	مقيد بشروط

حماية البيانات في الدول العربية

الاتجاهات الحديثة

شهدت السنوات الأخيرة توسعاً ملحوظاً في التشريعات العربية.

ومن الدول التي أصدرت قوانين متخصصة: السعودية والأردن والإمارات والبحرين وقطر ومصر.

التحديات المشتركة

تشمل: نقص الخبرات المتخصصة والتحول الرقمي السريع والذكاء الاصطناعي والحوسبة السحابية ونقل البيانات دولياً.

الحاجة إلى التنسيق الإقليمي

تزداد الحاجة إلى: توحيد المفاهيم القانونية وتطوير المعايير المشتركة وتسهيل انتقال البيانات بين الدول العربية وتعزيز التعاون الرقابي.

الذكاء الاصطناعي والتشريعات العربية

مع التوسع في استخدام الذكاء الاصطناعي أصبحت التشريعات العربية تواجه تحديات جديدة مثل: البيانات التدريبية مشروعية استخدام البيانات في تدريب النماذج والتوصيف الآلي اتخاذ القرارات المؤتمتة وتأثيرها على الحقوق الفردية والشفافية تفسير القرارات الصادرة عن الأنظمة الذكية والمسؤولية القانونية تحديد المسؤولية عند حدوث أخطاء أو أضرار.

مستقبل حماية البيانات في العالم العربي

من المتوقع أن تشهد السنوات القادمة: تطوير تشريعات أكثر تخصصاً وتنظيم الذكاء الاصطناعي بصورة مستقلة وزيادة العقوبات على الانتهاكات وتعزيز متطلبات الأمن السيبراني وإنشاء هيئات رقابية أكثر استقلالية ومواءمة أكبر مع المعايير الدولية.

كما يتوقع أن تصبح حماية البيانات أحد المتطلبات الأساسية للاستثمار والتعاون الدولي في المنطقة.

خاتمة الفصل

يمثل نظام حماية البيانات الشخصية السعودي (PDPL) أحد أبرز التشريعات العربية الحديثة في مجال حماية البيانات والخصوصية، وقد ساهم في تعزيز الإطار التنظيمي للاقتصاد الرقمي في المملكة. كما تظهر المقارنة بين النظام السعودي والقانون الأردني واللائحة الأوروبية GDPR وجود تقارب كبير في المبادئ الأساسية مع اختلافات تتعلق بالنطاق والآليات التنظيمية ومستوى النضج التشريعي.

ومع استمرار التطور التقني والاعتماد المتزايد على الذكاء الاصطناعي والبيانات الضخمة، ستصبح التشريعات العربية مطالبة بمواصلة التطوير لمواكبة التحديات الجديدة وضمان تحقيق التوازن بين الابتكار وحماية الحقوق الأساسية للأفراد.

الفصل الثالث عشر: قانون خصوصية المستهلك في كاليفورنيا **(CCPA/CPRA)** والتشريعات الأمريكية لحماية البيانات

مقدمة الفصل

على عكس الاتحاد الأوروبي الذي اعتمد إطاراً قانونياً موحداً لحماية البيانات من خلال اللائحة العامة لحماية البيانات(GDPR) ، اتبعت الولايات المتحدة نهجاً مختلفاً يقوم على تعدد القوانين والأنظمة التنظيمية وفقاً للقطاع أو الولاية. وقد أدى هذا النهج إلى ظهور مجموعة واسعة من القوانين التي تنظم حماية البيانات في مجالات محددة مثل الرعاية الصحية والخدمات المالية والتعليم.

ومع تزايد المخاوف المتعلقة بجمع البيانات الشخصية من قبل شركات التكنولوجيا الكبرى، أصدرت ولاية كاليفورنيا عام 2018 قانون خصوصية المستهلك في كاليفورنيا (California Consumer Privacy Act - CCPA)، والذي دخل حيز التنفيذ عام 2020. ثم تم تطويره لاحقاً من خلال قانون حقوق الخصوصية في كاليفورنيا(California Privacy Rights Act - CPRA) ، الذي عزز حقوق الأفراد ووسع الالتزامات المفروضة على الشركات.

ويُعد هذا التشريع من أكثر قوانين الخصوصية تأثيراً في الولايات المتحدة، نظراً للحجم الاقتصادي لولاية كاليفورنيا ووجود العديد من شركات التكنولوجيا العالمية فيها.

تطور حماية البيانات في الولايات المتحدة

النهج الأمريكي في حماية البيانات

تعتمد الولايات المتحدة على نظام تشريعي قطاعي(Sectoral Approach) ، حيث توجد قوانين مختلفة لكل مجال.

ومن الأمثلة:

القطاع الصحي

قانونHIPAA

القطاع المالي

قانونGLBA

حماية الأطفال

قانونCOPPA

التقارير الائتمانيةقانونFCRA

أسباب ظهورCCPA

شهدت السنوات الأخيرة عدة أحداث ساهمت في زيادة الضغط نحو إصدار تشريع شامل للخصوصية، منها: التوسع الهائل في جمع البيانات وفضائح تسريب البيانات واستغلال البيانات لأغراض سياسية وتسويقية وتصاعد مخاوف المستخدمين.

أهمية كاليفورنيا

تمثل ولاية كاليفورنيا: أكبر اقتصاد على مستوى الولايات الأمريكية ومقراً للعديد من شركات التكنولوجيا الكبرى ومركزاً عالمياً للابتكار الرقمي ولذلك فإن أي تشريع يصدر فيها يمتلك تأثيراً عالمياً واسعاً.

قانون خصوصية المستهلك في كاليفورنيا(CCPA)

أهداف القانون

يهدف CCPA إلى: تعزيز الشفافية ومنح المستهلكين مزيداً من السيطرة على بياناتهم وتنظيم ممارسات جمع البيانات وزيادة مساءلة الشركات.

نطاق التطبيق

ينطبق القانون على بعض الشركات التي تمارس أعمالها في كاليفورنيا وتستوفي معايير معينة تتعلق بحجم الإيرادات أو حجم البيانات التي تتم معالجتها.

مفهوم المستهلك

يعرف المستهلك بأنه: أي شخص طبيعي مقيم في ولاية كاليفورنيا وبغض النظر عن جنسيته.

مفهوم المعلومات الشخصية فيCCPA

يعتمد القانون تعريفاً واسعاً للمعلومات الشخصية ووتشمل: بيانات الهوية الاسم والعنوان والبريد الإلكتروني ورقم الهاتف والبيانات التجارية سجل المشتريات والسلوك الشرائي وتفضيلات المستهلك والبيانات التقنية عنوان IP وبيانات الأجهزة وسجل التصفح والبيانات الجغرافية الموقع الجغرافي وبيانات الحركة والبيانات البيومترية بصمة الوجه وبصمة الإصبع وبصمة الصوت.

حقوق المستهلكين

الحق في المعرفة

يحق للمستهلك معرفة: البيانات التي تم جمعها ومصادر البيانات وأغراض استخدامها والجهات التي تم الإفصاح لها عنها.

حق الوصول

الحصول على نسخة من البيانات الشخصية.

حق الحذف

طلب حذف البيانات الشخصية التي تم جمعها ومع وجود بعض الاستثناءات القانونية.

حق التصحيح

تم تعزيز هذا الحق لاحقاً بموجب CPRA ويتيح للمستهلك طلب تصحيح البيانات غير الدقيقة.

حق الاعتراض على بيع البيانات

يُعد هذا الحق من أهم الحقوق التي يتميز بها CCPA ويمنح الأفراد القدرة على منع بيع بياناتهم الشخصية للغير.

حق عدم التمييز

لا يجوز للشركات معاقبة الأفراد بسبب ممارستهم لحقوقهم القانونية ومثل: رفض تقديم الخدمة ورفع الأسعار بصورة تعسفية وتخفيض جودة الخدمة.

مفهوم بيع البيانات الشخصية

أهمية المفهوم

يمثل مفهوم بيع البيانات أحد أبرز الفروقات بين CCPA و.GDPR

تعريف البيع

يتبنى القانون مفهوماً واسعاً للبيع يشمل: البيع المباشر والتبادل التجاري ومشاركة البيانات مقابل منفعة اقتصادية.

خيار الانسحاب(Opt-Out)

يجب أن توفر الشركات آلية واضحة تسمح للمستهلكين بمنع بيع بياناتهم.

ويظهر ذلك غالباً من خلال رابط: Do Not Sell My Personal Information

قانون CPRA وتطوير CCPA

خلفية التعديل

في عام 2020 تم اعتماد CPRA لتطوير CCPA وتعزيز حماية الخصوصية.

البيانات الشخصية الحساسة

أدخل CPRA فئة جديدة هي: Sensitive Personal Information

وتشمل: البيانات الصحية والبيانات الجينية وبيانات الموقع الدقيق وبيانات الهوية الحكومية.

توسيع حقوق الأفراد

أضاف CPRA: حق التصحيح وحق تقييد استخدام البيانات الحساسة ومتطلبات إضافية للشفافية.

إنشاء جهة رقابية مستقلة

California Privacy Protection Agency (CPPA) للإشراف على تطبيق القانون.

التزامات الشركات

الشفافية

يجب توفير سياسة خصوصية واضحة تتضمن: أنواع البيانات المجمعة وأغراض المعالجة وحقوق المستهلك.

حماية البيانات

تطبيق تدابير أمنية مناسبة لحماية البيانات.

الاستجابة للطلبات

معالجة طلبات الأفراد خلال المدد القانونية المحددة.

الاحتفاظ بالسجلات

توثيق عمليات معالجة البيانات والطلبات الواردة من الأفراد.

العقوبات والمسؤوليات

العقوبات الإدارية

قد تفرض غرامات على الشركات المخالفة.

المسؤولية المدنية

يحق للأفراد رفع دعاوى في بعض حالات اختراق البيانات.

أثر العقوبات

تشجع العقوبات المؤسسات على: تحسين الامتثال وتعزيز الحوكمة والاستثمار في الأمن السيبراني.

مقارنة بين CCPA وGDPR

CCPA / CPRA	GDPR	العنصر
أقل تفصيلاً	مطلوب	الأساس القانوني للمعالجة
أقل اعتماداً	مركزية	الموافقة
موجود	واسع	حق الاعتراض
موجود	موجود	حق الحذف
موجود	موجود	حق نقل البيانات
عنصر رئيسي	غير مركزي	بيع البيانات
مرتبط بكاليفورنيا	عالمي	النطاق الجغرافي
أقل نسبياً	مرتفعة جداً	الغرامات

مقارنة مع القانون الأردني وPDPL

كاليفورنيا	السعودية	الأردن	العنصر
نعم	نعم	نعم	حقوق الوصول
نعم	نعم	نعم	حق الحذف

العنصر	الأردن	السعودية	كاليفورنيا
حق التصحيح	نعم	نعم	نعم
تنظيم بيع البيانات	محدود	محدود	متقدم
البيانات الحساسة	نعم	نعم	نعم
جهة رقابية مستقلة	موجودة	موجودة	موجودة

أثر التشريعات الأمريكية على شركات التكنولوجيا

أثرت CCPA و CPRAبصورة كبيرة على الشركات العالمية.

ومن أبرز الآثار: تحديث سياسات الخصوصية أجبرت الشركات على مراجعة سياساتها وإجراءاتها وتعزيز الشفافية زيادة الإفصاح عن كيفية استخدام البيانات وتطوير أدوات الخصوصية إضافة أدوات لإدارة الموافقات والطلبات والاستثمار في الامتثال إنشاء فرق قانونية وتقنية متخصصة.

الذكاء الاصطناعي والخصوصية في الولايات المتحدة مع انتشار الذكاء الاصطناعي أصبحت هناك قضايا جديدة مثل: البيانات التدريبية كيفية استخدام البيانات في تدريب النماذج والتحيز الخوارزمي التأكد من عدم التمييز ضد الأفراد والشفافية فهم آليات اتخاذ القرار داخل الأنظمة الذكية والمساءلة تحديد المسؤولية عن الأخطاء الناتجة عن الذكاء الاصطناعي.

خاتمة الفصل

يمثل قانون خصوصية المستهلك في كاليفورنيا (CCPA) وتعديلاته اللاحقة (CPRA) خطوة مهمة في تطوير حماية البيانات داخل الولايات المتحدة، وقد ساهم في تعزيز حقوق الأفراد وزيادة مساءلة الشركات. كما أن تأثيره تجاوز حدود ولاية كاليفورنيا ليؤثر في سياسات الخصوصية لدى العديد من الشركات العالمية.

وتظهر المقارنة بين CCPA و GDPRوالقوانين العربية أن هناك اتجاهاً عالمياً متزايداً نحو تعزيز حقوق الأفراد وفرض التزامات أكبر على الجهات التي تجمع البيانات وتعالجها، مع استمرار ظهور تحديات جديدة مرتبطة بالذكاء الاصطناعي والاقتصاد الرقمي.

الفصل الرابع عشر: قانون الذكاء الاصطناعي الأوروبي(EU AI Act)

مقدمة الفصل

يُعد قانون الذكاء الاصطناعي الأوروبي (European Union Artificial Intelligence Act - EU AI Act) أول إطار قانوني شامل في العالم يهدف إلى تنظيم تطوير واستخدام أنظمة الذكاء الاصطناعي على نطاق واسع. وقد جاء هذا التشريع استجابة للنمو المتسارع لتقنيات الذكاء الاصطناعي وتأثيرها المتزايد على الأفراد والمؤسسات والمجتمعات، وما يرتبط بها من فرص اقتصادية كبيرة ومخاطر قانونية وأخلاقية وأمنية.

ويهدف القانون إلى تحقيق توازن دقيق بين تشجيع الابتكار التقني من جهة، وضمان حماية الحقوق الأساسية للأفراد من جهة أخرى. وعلى غرار اللائحة العامة لحماية البيانات(GDPR) ، يتوقع أن يكون لهذا القانون تأثير عالمي واسع يتجاوز حدود الاتحاد الأوروبي، نظراً لأهمية السوق الأوروبية واعتماد العديد من الشركات العالمية على تقديم خدماتها داخل دول الاتحاد.

ويكتسب هذا القانون أهمية خاصة في عصر الذكاء الاصطناعي التوليدي، حيث أصبحت النماذج الذكية قادرة على اتخاذ قرارات مؤثرة وإنتاج محتوى معقد والتفاعل مع المستخدمين بطرق لم تكن ممكنة سابقاً.

خلفية إصدار قانون الذكاء الاصطناعي الأوروبي

التطور السريع للذكاء الاصطناعي

شهد العقد الأخير تطوراً غير مسبوق في قدرات الذكاء الاصطناعي، خصوصاً في مجالات: معالجة اللغة الطبيعية والرؤية الحاسوبية والمركبات الذاتية القيادة والتحليلات التنبؤية والذكاء الاصطناعي التوليدي.

وقد أدى ذلك إلى ظهور تحديات تتعلق بالخصوصية والتمييز والشفافية والمساءلة.

الحاجة إلى التنظيم

قبل صدور القانون لم يكن هناك إطار قانوني أوروبي موحد ينظم الذكاء الاصطناعي بشكل مباشر.

وكانت القوانين القائمة تركز على: حماية البيانات وحقوق المستهلك والأمن السيبراني والمسؤولية المدنية ولكنها لم تكن كافية لمعالجة المخاطر الخاصة بالأنظمة الذكية.

أهداف القانون

يسعى القانون إلى: حماية الحقوق الأساسية وتعزيز الثقة في الذكاء الاصطناعي ودعم الابتكار المسؤول ومنع الاستخدامات الضارة وتوحيد القواعد التنظيمية داخل الاتحاد الأوروبي.

مفهوم نظام الذكاء الاصطناعي

تعريف النظام

يعرف القانون نظام الذكاء الاصطناعي بأنه:

نظام آلي مصمم للعمل بدرجات متفاوتة من الاستقلالية، وقادر على استنتاج كيفية إنتاج مخرجات مثل التنبؤات أو القرارات أو التوصيات أو المحتوى المؤثر في البيئات المادية أو الافتراضية.

نطاق الأنظمة المشمولة

يشمل القانون: نماذج الذكاء الاصطناعي التوليدي وأنظمة اتخاذ القرار المؤتمت وأنظمة التعرف على الصور وأنظمة تحليل الصوت وأنظمة التصنيف والتنبؤ.

الجهات الخاضعة للقانون

يشمل القانون: مطوري الأنظمة ومزودي الخدمات والمستوردين والموزعين والمستخدمين المؤسسيين.

النهج القائم على المخاطر

يُعد تصنيف المخاطر الركيزة الأساسية للقانون وويتم تقسيم أنظمة الذكاء الاصطناعي إلى أربع فئات رئيسية.

الأنظمة ذات المخاطر غير المقبولة

مفهومها

تمثل الأنظمة التي يعتبرها الاتحاد الأوروبي تهديداً مباشراً للحقوق والحريات الأساسية.

ولذلك يتم حظرها بالكامل.

أمثلة على الأنظمة المحظورة

التلاعب السلوكي الأنظمة التي تستغل نقاط الضعف النفسية للأفراد والاستغلال الموجه للأطفال الأنظمة التي تؤثر على سلوك الأطفال بصورة ضارة.

التقييم الاجتماعي(Social Scoring) أنظمة تصنيف الأفراد بناءً على سلوكهم أو خصائصهم الشخصية بصورة تؤثر على حقوقهم.

بعض أشكال المراقبة البيومترية خصوصاً الاستخدامات واسعة النطاق وغير المتناسبة.

مفهوم الأنظمة عالية المخاطر

هي الأنظمة التي قد تؤثر بصورة جوهرية على: الحقوق الأساسية والسلامة العامة وفرص العمل والتعليم والخدمات الأساسية.

المجالات المصنفة عالية المخاطر

التوظيف أنظمة تقييم المتقدمين للوظائف والتعليم أنظمة تقييم الطلاب واتخاذ القرارات التعليمية والرعاية الصحية أنظمة دعم التشخيص والعلاج والخدمات المالية أنظمة منح القروض والتقييم الائتماني والبنية التحتية الحيوية أنظمة الطاقة والمياه والنقل والعدالة وإنفاذ القانون بعض الأنظمة المستخدمة في التحقيقات والإجراءات القانونية ومتطلبات الأنظمة عالية المخاطر يفرض القانون مجموعة من الالتزامات الصارمة.

إدارة المخاطر

يجب إنشاء نظام متكامل لتقييم المخاطر ومراقبتها طوال دورة حياة النظام.

جودة البيانات

يجب أن تكون البيانات المستخدمة: دقيقة ومناسبة وممثلة للواقع وخالية قدر الإمكان من التحيز.

التوثيق الفني

يجب الاحتفاظ بوثائق تفصيلية تشمل: تصميم النظام ومصادر البيانات وآليات العمل ونتائج الاختبارات.

الشفافية

يجب توفير معلومات كافية للمستخدمين لفهم طبيعة النظام وحدوده.

الإشراف البشري

ينبغي ألا تعمل الأنظمة عالية المخاطر بصورة مستقلة بالكامل دون إمكانية التدخل البشري.

الأمن السيبراني

يجب حماية الأنظمة من: الاختراق والتلاعب وتسميم البيانات وإساءة الاستخدام.

الأنظمة محدودة المخاطر تشمل الأنظمة التي لا تشكل خطراً كبيراً ولكنها تتطلب شفافية معينة.

أمثلة روبوتات المحادثة والمساعدات الذكية ومولدات الصور والالتزام الأساسي يجب إعلام المستخدم بأنه يتفاعل مع نظام ذكاء اصطناعي.

الأنظمة منخفضة المخاطر

تشمل التطبيقات اليومية البسيطة.

مثل: فلاتر البريد المزعج وأنظمة التوصية البسيطة وبعض الألعاب الذكية وولا تخضع لالتزامات تنظيمية واسعة.

تنظيم الذكاء الاصطناعي التوليدي

ظهور النماذج التوليدية

مع ظهور:

- GPT
- Gemini
- Claude
- Llama
- Mistral

أصبح من الضروري وضع قواعد خاصة بالنماذج التوليدية.

متطلبات الشفافية

يجب على مزودي النماذج: الإفصاح عن كون المحتوى مولداً بواسطة الذكاء الاصطناعي عند الحاجة وتوضيح قدرات النظام وحدوده واتخاذ تدابير للحد من المحتوى الضار.

حقوق الملكية الفكرية

يتطلب القانون توفير معلومات حول استخدام المواد المحمية بحقوق النشر في التدريب.

النماذج الأساسية(Foundation Models)

مفهومها

هي النماذج واسعة النطاق القابلة للتكيف مع العديد من المهام.

أمثلة

- GPT
- Gemini
- Claude

- Llama
- Qwen

الالتزامات الخاصة

تشمل: تقييم المخاطر والتوثيق والشفافية والأمن السيبراني.

الحادي عشر: العلاقة بين AI Act وGDPR

أوجه التكامل

يعالج GDPR: البيانات الشخصية والخصوصية وحقوق الأفراد وبينما يعالج AI Act: مخاطر الذكاء الاصطناعي والسلامة والشفافية والحوكمة.

العلاقة العملية عند استخدام بيانات شخصية داخل نظام ذكاء اصطناعي يجب الامتثال لكلا التشريعين معاً.

العقوبات يفرض القانون عقوبات كبيرة على المخالفات.

وقد تصل في بعض الحالات الخطيرة إلى: عشرات الملايين من اليورو وأو نسبة من الإيرادات العالمية السنوية للشركة وتختلف العقوبات حسب نوع المخالفة وخطورتها.

الثالث عشر: أثر القانون على المؤسسات

سيؤثر القانون على: شركات التكنولوجيا من خلال متطلبات التوثيق والشفافية والمؤسسات المالية من خلال تنظيم أنظمة اتخاذ القرار المؤتمت والقطاع الصحي من خلال تنظيم الأنظمة الطبية الذكية والمؤسسات التعليمية من خلال تنظيم أنظمة تقييم الطلبة والجهات الحكومية من خلال ضبط استخدام الذكاء الاصطناعي في الخدمات العامة.

أثر القانون على العالم العربي

رغم أن القانون أوروبي، إلا أن تأثيره يمتد إلى المؤسسات العربية التي: تقدم خدمات داخل أوروبا وتتعامل مع مواطنين أوروبيين وتستخدم مزودي خدمات أوروبيين وتطور أنظمة ذكاء اصطناعي موجهة للأسواق الأوروبية.

ومن المتوقع أن يؤثر في تطوير التشريعات العربية المستقبلية المتعلقة بالذكاء الاصطناعي.

الخامس عشر: مستقبل تنظيم الذكاء الاصطناعي

يمثل AI Act بداية مرحلة جديدة من التنظيم العالمي للذكاء الاصطناعي.

ومن المتوقع خلال السنوات القادمة ظهور: قوانين وطنية مماثلة ومعايير دولية موحدة ومتطلبات أكثر صرامة للشفافية وضوابط خاصة بالذكاء الاصطناعي العام (AGI).

خاتمة الفصل

يُعد قانون الذكاء الاصطناعي الأوروبي (EU AI Act) أول محاولة شاملة لتنظيم الذكاء الاصطناعي على المستوى العالمي. وقد تبنى نهجاً قائماً على تقييم المخاطر يوازن بين تشجيع الابتكار وحماية الحقوق الأساسية للأفراد. كما وضع قواعد جديدة لتنظيم الأنظمة عالية المخاطر والنماذج التوليدية والنماذج الأساسية، مما يجعله مرجعاً رئيسياً للتشريعات المستقبلية في هذا المجال.

ومع استمرار التطور السريع للذكاء الاصطناعي، سيشكل هذا القانون نقطة تحول تاريخية في العلاقة بين التكنولوجيا والقانون والأخلاقيات.

الفصل الخامس عشر: أخلاقيات الذكاء الاصطناعي وحماية البيانات

مقدمة الفصل

شهد العالم خلال العقد الأخير توسعاً غير مسبوق في استخدام أنظمة الذكاء الاصطناعي في مختلف المجالات الاقتصادية والاجتماعية والتعليمية والصحية والأمنية. وقد أسهمت هذه الأنظمة في تحسين الإنتاجية وتطوير الخدمات واتخاذ القرارات بصورة أكثر سرعة وكفاءة. إلا أن هذا التطور المتسارع صاحبه ظهور مجموعة من التساؤلات الأخلاقية المتعلقة بكيفية تصميم هذه الأنظمة وتدريبها واستخدامها وتأثيرها على الأفراد والمجتمعات.

وفي حين تركز التشريعات القانونية على تحديد ما هو مسموح أو ممنوع، فإن الأخلاقيات تهتم بما هو صحيح وعادل ومسؤول. ولذلك أصبحت أخلاقيات الذكاء الاصطناعي أحد المحاور الأساسية في النقاشات العالمية المتعلقة بمستقبل التكنولوجيا وحماية البيانات والحقوق الرقمية.

وتزداد أهمية البعد الأخلاقي في ظل اعتماد أنظمة الذكاء الاصطناعي على كميات ضخمة من البيانات الشخصية، وقدرتها المتزايدة على التأثير في القرارات البشرية والسلوك الاجتماعي.

يهدف هذا الفصل إلى دراسة المبادئ الأخلاقية المرتبطة بالذكاء الاصطناعي وحماية البيانات وتحليل التحديات الأخلاقية التي تواجه المؤسسات والمجتمعات في عصر الذكاء الاصطناعي التوليدي.

مفهوم أخلاقيات الذكاء الاصطناعي

تعريف الأخلاقيات

الأخلاقيات (Ethics) هي مجموعة المبادئ والقيم التي تساعد على التمييز بين السلوك الصحيح والخاطئ.

وتهدف إلى توجيه القرارات والأفعال بما يحقق العدالة والمصلحة العامة واحترام الإنسان.

مفهوم أخلاقيات الذكاء الاصطناعي

مجموعة المبادئ والقيم والمعايير التي تهدف إلى ضمان تصميم وتطوير واستخدام أنظمة الذكاء الاصطناعي بطريقة مسؤولة وعادلة وآمنة وتحترم حقوق الإنسان.

أهمية الأخلاقيات في الذكاء الاصطناعي

تنبع أهمية الأخلاقيات من قدرة الأنظمة الذكية على: اتخاذ قرارات مؤثرة وتحليل السلوك البشري وجمع البيانات الشخصية والتأثير على الرأي العام وأتمتة العديد من الوظائف والخدمات.

مبدأ العدالة وعدم التحيز

مفهوم العدالة

يقصد بالعدالة ضمان معاملة جميع الأفراد بصورة منصفة ومتساوية دون تمييز غير مبرر.

التحيز في الذكاء الاصطناعي

قد تتأثر الأنظمة الذكية بالتحيزات الموجودة في البيانات المستخدمة أثناء التدريب.

ومن أمثلة ذلك: التحيز العرقي والتحيز الجندري والتحيز الاجتماعي والتحيز الاقتصادي.

مصادر التحيز

البيانات عندما تكون البيانات غير ممثلة لجميع الفئات والخوارزميات عندما تتضمن النماذج افتراضات تؤدي إلى نتائج غير عادلة والمستخدمون عندما يتم استخدام الأنظمة بصورة غير موضوعية.

آثار التحيز

قد يؤدي التحيز إلى: رفض طلبات التوظيف بصورة غير عادلة وتمييز في منح القروض وأخطاء في التشخيص الطبي وتقييد الفرص التعليمية.

مفهوم الشفافية

تعني الشفافية قدرة الأفراد على معرفة: كيف يعمل النظام وكيف يتم استخدام البيانات وكيف يتم اتخاذ القرارات.

أهمية الشفافية

تساعد على: تعزيز الثقة وتحسين المساءلة وحماية الحقوق الفردية وكشف الأخطاء والتحيزات.

قابلية التفسير

يقصد بها قدرة الإنسان على فهم أسباب القرار الذي اتخذه النظام.

مشكلة الصندوق الأسود

تعاني بعض النماذج المتقدمة من مشكلة تعرف باسم: Black Box Problem

حيث يصعب تفسير كيفية وصول النموذج إلى نتيجة معينة وهذا يمثل تحدياً أخلاقياً وقانونياً كبيراً.

مفهوم المساءلة

تعني إمكانية تحديد الجهة المسؤولة عن نتائج النظام الذكي.

أهمية المساءلة

تضمن: معالجة الأخطاء وتعويض المتضررين وتحسين الأنظمة ومنع إساءة الاستخدام.

سؤال المسؤولية

من أبرز الأسئلة الأخلاقية المعاصرة:

من المسؤول إذا تسبب نظام ذكاء اصطناعي في ضرر؟

هل هو:

- المطور؟
- الشركة المالكة؟
- المستخدم؟
- مزود البيانات؟

المسؤولية المشتركة

تميل معظم الأطر الحديثة إلى اعتبار المسؤولية مشتركة بين جميع الأطراف المشاركة في تطوير واستخدام النظام.

مفهوم الكرامة الإنسانية

تمثل الكرامة الإنسانية أحد المبادئ الأساسية في جميع المواثيق الدولية لحقوق الإنسان.

الذكاء الاصطناعي والكرامة

ينبغي ألا تؤدي الأنظمة الذكية إلى: إذلال الأفراد وانتهاك الخصوصية والتمييز وتقييد الحريات الأساسية.

الاستقلالية البشرية

يقصد بها قدرة الإنسان على اتخاذ قراراته بحرية.

ويجب ألا تؤدي الأنظمة الذكية إلى سلب هذه القدرة أو التأثير عليها بصورة غير مشروعة.

أخلاقيات البيانات الضخمة

جمع البيانات

من الأسئلة الأخلاقية المهمة:

- هل تم جمع البيانات بموافقة حقيقية؟
- هل يفهم الأفراد كيفية استخدامها؟

استخدام البيانات

ينبغي أن يكون الاستخدام: مشروعاً وعادلاً ومتناسباً مع الغرض.

تقليل البيانات

من المبادئ الأخلاقية الأساسية:

جمع أقل كمية ممكنة من البيانات اللازمة لتحقيق الهدف.

الاحتفاظ بالبيانات

يجب عدم الاحتفاظ بالبيانات لفترات غير مبررة.

الذكاء الاصطناعي التوليدي والتحديات الأخلاقية

المحتوى المولد آلياً

أصبحت النماذج التوليدية قادرة على إنتاج: نصوص وصور وفيديو وأصوات وبدرجة عالية من الواقعية.

التزييف العميق

يعد التزييف العميق من أبرز التحديات الأخلاقية وإذ يمكن استخدامه في: التضليل الإعلامي والاحتيال والابتزاز وانتحال الهوية.

المعلومات المضللة

قد تنتج النماذج محتوى: غير دقيق ومضلل ومختلق.

وهو ما يعرف أحياناً باسم Hallucinations

حقوق الملكية الفكرية

يثير الذكاء الاصطناعي التوليدي أسئلة مهمة حول: حقوق المؤلف وملكية المحتوى واستخدام المواد التدريبية.

أخلاقيات الذكاء الاصطناعي في القطاعات المختلفة

القطاع الصحي

يجب ضمان: سلامة المرضى ودقة القرارات وحماية البيانات الصحية.

القطاع المالي

يجب منع: التمييز والقرارات غير العادلة وإساءة استخدام البيانات المالية.

القطاع التعليمي

يجب مراعاة: العدالة بين الطلبة وحماية البيانات التعليمية وعدم الاعتماد الكامل على القرارات الآلية.

القطاع الحكومي

يجب تحقيق التوازن بين: الكفاءة والأمن وحقوق المواطنين.

المبادئ العالمية لأخلاقيات الذكاء الاصطناعي

اعتمدت العديد من المنظمات الدولية مجموعة من المبادئ المشتركة.

ومن أبرزها: منظمة اليونسكو احترام حقوق الإنسان والعدالة والشمول والاستدامة ومنظمة التعاون الاقتصادي والتنمية (OECD) الشفافية والمساءلة والسلامة والاستدامة والاتحاد الأوروبي الرقابة البشرية والشفافية والعدالة والخصوصية.

بناء إطار أخلاقي مؤسسي

أهمية الحوكمة الأخلاقية

لا يكفي الامتثال القانوني وحده لضمان الاستخدام المسؤول للذكاء الاصطناعي.

عناصر الإطار الأخلاقي

السياسات وضع سياسات واضحة لاستخدام الذكاء الاصطناعي واللجان الأخلاقية إنشاء لجان لمراجعة المشاريع عالية المخاطر وتقييم التأثير تحليل الآثار الأخلاقية قبل إطلاق الأنظمة والمراجعة المستمرة متابعة الأداء واكتشاف الانحرافات.

ثقافة المسؤولية

يجب أن تصبح الأخلاقيات جزءاً من الثقافة المؤسسية وليس مجرد متطلب تنظيمي.

العلاقة بين الأخلاق والقانون على الرغم من وجود علاقة وثيقة بين القانون والأخلاق، فإنهما ليسا شيئاً واحداً.

القانون	الأخلاق
يركز على ما هو مسموح	تركز على ما هو صحيح
أكثر تحديداً	أوسع نطاقاً
تعتمد على النصوص القانونية	تعتمد على القيم
تحدد الحد الأدنى للالتزام	قد تتجاوز المتطلبات القانونية

ولهذا السبب قد يكون بعض السلوك قانونياً لكنه غير أخلاقي.

مستقبل أخلاقيات الذكاء الاصطناعي

من المتوقع أن تشهد السنوات القادمة: زيادة التركيز على الذكاء الاصطناعي المسؤول وتطوير معايير أخلاقية عالمية وتعزيز الشفافية وقابلية التفسير وتوسيع الرقابة على الأنظمة عالية المخاطر ودمج الأخلاقيات في مراحل التصميم والتطوير.

كما ستصبح الأخلاقيات عاملاً رئيسياً في تقييم نجاح الأنظمة الذكية وقبولها مجتمعياً.

خاتمة الفصل

تمثل أخلاقيات الذكاء الاصطناعي الإطار القيمي الذي يوجه تطوير واستخدام الأنظمة الذكية بصورة تحترم الإنسان وحقوقه الأساسية. ومع تزايد الاعتماد على البيانات والذكاء الاصطناعي التوليدي، أصبحت قضايا العدالة والشفافية والمساءلة والخصوصية أكثر أهمية من أي وقت مضى.

ولا يمكن تحقيق الاستفادة الكاملة من الذكاء الاصطناعي دون بناء أنظمة تجمع بين الكفاءة التقنية والمسؤولية الأخلاقية، وتضع الإنسان في مركز عملية التطوير واتخاذ القرار.

الفصل السادس عشر: حوكمة الذكاء الاصطناعي وإدارة الامتثال المؤسسي

مقدمة الفصل

أصبح الذكاء الاصطناعي جزءاً أساسياً من استراتيجيات التحول الرقمي في المؤسسات الحكومية والخاصة، وأداة رئيسية لتحسين الكفاءة التشغيلية واتخاذ القرارات وتطوير الخدمات. ومع تزايد الاعتماد على الأنظمة الذكية، ظهرت الحاجة إلى إنشاء أطر حوكمة متخصصة تضمن الاستخدام المسؤول والآمن والقانوني لهذه التقنيات.

وتشير حوكمة الذكاء الاصطناعي إلى مجموعة السياسات والإجراءات والهياكل التنظيمية التي تضمن تطوير واستخدام الذكاء الاصطناعي بطريقة تتوافق مع القوانين والمعايير الأخلاقية ومتطلبات الأمن والخصوصية.

وفي ظل التحديات المرتبطة بالتحيز والشفافية والخصوصية والمسؤولية القانونية، أصبحت الحوكمة عاملاً أساسياً لتحقيق الثقة والاستدامة في مشاريع الذكاء الاصطناعي.

يهدف هذا الفصل إلى دراسة مفهوم حوكمة الذكاء الاصطناعي وأهم الأطر والمعايير الدولية ذات الصلة، واستعراض أفضل الممارسات المؤسسية لبناء برامج حوكمة فعالة.

مفهوم حوكمة الذكاء الاصطناعي

تعريف الحوكمة

تشير الحوكمة (Governance) إلى:

مجموعة القواعد والسياسات والهياكل التنظيمية التي تضمن إدارة الأنشطة والموارد بصورة فعالة ومسؤولة وشفافة.

تعريف حوكمة الذكاء الاصطناعي

الإطار المؤسسي الذي يحدد كيفية تصميم وتطوير ونشر واستخدام ومراقبة أنظمة الذكاء الاصطناعي بما يضمن الامتثال القانوني والأخلاقي والتقني.

أهداف الحوكمة

تهدف حوكمة الذكاء الاصطناعي إلى: حماية الحقوق الأساسية وتعزيز الثقة في الأنظمة الذكية وإدارة المخاطر وضمان الامتثال القانوني وتعزيز الشفافية والمساءلة ودعم الابتكار المسؤول.

أهمية الحوكمة في عصر الذكاء الاصطناعي

تعقيد الأنظمة الحديثة

تتميز الأنظمة الذكية الحديثة بما يلي: التعلم الذاتي واتخاذ القرارات المؤتمتة وتحليل البيانات الضخمة والتفاعل مع البشر ومما يجعل إدارتها أكثر تعقيداً من الأنظمة التقليدية.

المخاطر المؤسسية

قد تؤدي الأنظمة الذكية إلى: أخطاء تشغيلية وتحيزات غير مقصودة وانتهاكات للخصوصية ومسؤوليات قانونية وخسائر مالية.

المتطلبات التنظيمية

تتزايد المتطلبات التنظيمية المرتبطة بـ: GDPR وAI Act وPDPL وقوانين حماية البيانات الوطنية ومما يجعل الحوكمة ضرورة استراتيجية.

مبادئ حوكمة الذكاء الاصطناعي

الشفافية

يجب أن تكون عمليات الذكاء الاصطناعي: قابلة للفهم وموثقة وقابلة للتفسير عند الحاجة.

العدالة

ينبغي تقليل احتمالية التحيز والتمييز.

المساءلة

يجب تحديد المسؤوليات بوضوح.

الخصوصية

احترام البيانات الشخصية وحمايتها.

الأمن

ضمان مقاومة الأنظمة للهجمات والتلاعب.

الرقابة البشرية

الحفاظ على دور الإنسان في الإشراف واتخاذ القرار.

معيار ISO 42001

مقدمة

يُعد معيار ISO/IEC 42001 أول معيار دولي متخصص في نظم إدارة الذكاء الاصطناعي.

وقد صدر عن المنظمة الدولية للتقييس (ISO) بهدف توفير إطار عملي لإدارة أنظمة الذكاء الاصطناعي.

أهداف المعيار

يساعد المعيار المؤسسات على: إدارة مخاطر الذكاء الاصطناعي وتعزيز الامتثال وتحسين الشفافية ودعم الحوكمة.

مكونات النظام

يتضمن المعيار: القيادة التزام الإدارة العليا والتخطيط تحديد المخاطر والأهداف والتشغيل إدارة دورة حياة الأنظمة والتقييم قياس الأداء والامتثال والتحسين التطوير المستمر.

إطار NIST لإدارة مخاطر الذكاء الاصطناعي

نبذة عن الإطار

طور المعهد الوطني الأمريكي للمعايير والتقنية (NIST) إطاراً لإدارة مخاطر الذكاء الاصطناعي.

ويهدف إلى مساعدة المؤسسات على إدارة المخاطر بطريقة منهجية.

الوظائف الرئيسية للإطار

الحوكمة (Govern) وضع السياسات والمسؤوليات والتحديد (Map) فهم السياق والمخاطر والقياس (Measure) تحليل المخاطر وتقييمها والإدارة (Manage) تنفيذ الإجراءات التصحيحية.

أهمية الإطار

يوفر مرونة عالية للمؤسسات بمختلف أحجامها وقطاعاتها.

إدارة الامتثال المؤسسي

مفهوم الامتثال

التزام المؤسسة بالقوانين واللوائح والمعايير والسياسات الداخلية.

عناصر برنامج الامتثال

السياسات وضع سياسات مكتوبة وواضحة والتدريب رفع وعي الموظفين والمراقبة متابعة الالتزام المستمر والتدقيق إجراء مراجعات دورية.

الذكاء الاصطناعي والامتثال

ينبغي التأكد من توافق الأنظمة الذكية مع: قوانين حماية البيانات والمتطلبات القطاعية والسياسات الداخلية.

تقييم أثر الذكاء الاصطناعي(AI Impact Assessment)

مفهوم التقييم

هو عملية منهجية لتحديد الآثار المحتملة لنظام الذكاء الاصطناعي قبل تشغيله.

أهداف التقييم

تحديد المخاطر وتقييم الأثر على الأفراد وتحسين الشفافية ودعم اتخاذ القرار.

عناصر التقييم

وصف النظام ما وظيفة النظام؟

البيانات المستخدمة ما نوع البيانات؟

الأطراف المتأثرة من سيتأثر بالقرارات؟

تحليل المخاطر ما المخاطر المحتملة؟

إجراءات التخفيف كيف يمكن تقليل المخاطر؟

إدارة مخاطر الذكاء الاصطناعي

أنواع المخاطر

المخاطر القانونية مثل انتهاك قوانين الخصوصية والمخاطر التشغيلية مثل الأعطال أو الأخطاء والمخاطر الأخلاقية مثل التحيز وعدم العدالة والمخاطر الأمنية مثل الاختراق أو تسميم البيانات ومخاطر السمعة فقدان ثقة العملاء أو الجمهور.

دورة إدارة المخاطر

تتكون من: التحديد والتقييم والمعالجة والمراقبة والتحسين.

الهيكل التنظيمي للحوكمة

مجلس الإدارة

يتحمل المسؤولية النهائية عن الحوكمة.

الإدارة التنفيذية

تشرف على تنفيذ السياسات.

مسؤول حماية البيانات

يتابع الامتثال المتعلق بالخصوصية.

فريق الذكاء الاصطناعي

يتولى التطوير والتشغيل.

التدقيق الداخلي

يقوم بالمراجعة المستقلة.

دورة حياة حوكمة الذكاء الاصطناعي

التخطيط تحديد الأهداف والمخاطر والتصميم دمج الخصوصية والأمن والأخلاقيات والتطوير بناء واختبار النماذج والنشر تشغيل الأنظمة في البيئة الفعلية والمراقبة متابعة الأداء والمخاطر والتحسين تحديث النماذج والإجراءات.

بناء برنامج حوكمة متكامل يتكون البرنامج الناجح من: سياسة ذكاء اصطناعي مؤسسية تحدد القواعد العامة وسجل الأنظمة الذكية حصر جميع الأنظمة المستخدمة وتصنيف المخاطر تحديد الأنظمة عالية ومتوسطة ومنخفضة المخاطر وتقييمات دورية مراجعة مستمرة للمخاطر والامتثال ولجان الحوكمة الإشراف على المشاريع الحساسة وإدارة الحوادث التعامل مع المشكلات والانتهاكات.

حوكمة الذكاء الاصطناعي في المؤسسات العربية

تواجه المؤسسات العربية تحديات تشمل: نقص الخبرات المتخصصة وحداثة التشريعات وسرعة التحول الرقمي ومحدودية الأطر التنظيمية المحلية.

وفي المقابل تتيح هذه المرحلة فرصة لبناء أطر حوكمة حديثة منذ البداية بالاستفادة من أفضل الممارسات العالمية.

مستقبل حوكمة الذكاء الاصطناعي

من المتوقع أن تصبح حوكمة الذكاء الاصطناعي خلال السنوات القادمة جزءاً أساسياً من: الحوكمة المؤسسية وإدارة المخاطر والامتثال التنظيمي والأمن السيبراني والاستدامة الرقمية.

كما سيزداد الاعتماد على معايير دولية مثل:

- ISO 42001
- ISO 27001
- ISO 27701
- NIST AI RMF

لتوفير إطار موحد لإدارة الذكاء الاصطناعي بصورة مسؤولة.

خاتمة الفصل

تمثل حوكمة الذكاء الاصطناعي حجر الأساس للاستخدام المسؤول والآمن للتقنيات الذكية داخل المؤسسات. فهي لا تقتصر على الامتثال للقوانين فحسب، بل تمتد إلى إدارة المخاطر وتعزيز الشفافية والمساءلة وحماية الخصوصية وضمان العدالة. ومع تزايد تعقيد الأنظمة الذكية وتوسع استخدامها، ستصبح الحوكمة الفعالة شرطاً أساسياً لتحقيق الثقة والاستدامة والنجاح في عصر الذكاء الاصطناعي.

الفصل السابع عشر: الخصوصية وحماية البيانات في **ChatGPT** و **Claude**و **Gemini**و**Copilot**

مقدمة الفصل

أحدثت أدوات الذكاء الاصطناعي التوليدي تحولاً جذرياً في طريقة تعامل الأفراد والمؤسسات مع المعلومات والمعرفة والإنتاج الرقمي. فقد أصبحت منصات مثل ChatGPT و Claudeو Gemini و Microsoft Copilotجزءاً من بيئات العمل والتعليم والبحث العلمي وتطوير البرمجيات، حيث توفر قدرات متقدمة في إنشاء المحتوى وتحليل البيانات والإجابة عن الأسئلة وتنفيذ المهام المعرفية المعقدة.

ورغم الفوائد الكبيرة لهذه الأدوات، فإن استخدامها يثير العديد من القضايا المتعلقة بالخصوصية وحماية البيانات، خصوصاً عند إدخال معلومات شخصية أو مؤسسية حساسة إلى هذه الأنظمة. وتزداد أهمية هذه القضايا في ظل اعتماد هذه النماذج على الحوسبة السحابية، ووجود سياسات مختلفة لإدارة البيانات والتدريب والاحتفاظ بالمعلومات.

يهدف هذا الفصل إلى دراسة الجوانب المتعلقة بالخصوصية وحماية البيانات في أشهر منصات الذكاء الاصطناعي التوليدي، وتحليل المخاطر المرتبطة باستخدامها، وتقديم مجموعة من الإرشادات العملية للمؤسسات والأفراد.

كيف تعمل نماذج الذكاء الاصطناعي التوليدي؟

مفهوم النماذج التوليدية

تعتمد النماذج التوليدية على تقنيات التعلم العميق ونماذج اللغة الكبيرة(LLMs) ، حيث يتم تدريبها على كميات ضخمة من البيانات النصية والمرئية والصوتية.

وتهدف هذه النماذج إلى: فهم اللغة الطبيعية وتوليد محتوى جديد وتحليل المعلومات وتنفيذ التعليمات.

مراحل العمل الأساسية

تمر عملية التفاعل مع النموذج عادة بالمراحل التالية:

إدخال البيانات

يقوم المستخدم بإرسال: نص وملف وصورة وصوت والمعالجة يتم تحليل المدخلات بواسطة النموذج وتوليد الاستجابة يقوم النظام بإنشاء مخرجات جديدة بناءً على الأنماط التي تعلمها.

التخزين والإدارة قد يتم الاحتفاظ ببعض البيانات وفقاً لسياسات الخدمة وإعدادات المستخدم.

أنواع البيانات التي تتم معالجتها

البيانات النصية

تشمل: الأسئلة والمحادثات والمستندات والتقارير.

البيانات المرئية

مثل: الصور والمخططات ولقطات الشاشة.

الملفات

قد تشمل:

- PDF
- Word
- Excel
- PowerPoint

البيانات الوصفية

مثل: وقت الاستخدام والجهاز المستخدم والموقع التقريبي وإعدادات الحساب.

الخصوصية وحماية البيانات في ChatGPT

نظرة عامة

يُعد ChatGPT أحد أشهر تطبيقات الذكاء الاصطناعي التوليدي في العالم، ويعتمد على نماذج GPT المطورة من قبل شركة OpenAI.

البيانات التي تتم معالجتها

قد تشمل: المحادثات النصية والملفات المرفوعة والصور والتعليمات المخصصة.

إعدادات الخصوصية

توفر المنصة خيارات لإدارة البيانات مثل: إدارة سجل المحادثات والتحكم في استخدام البيانات لتحسين النماذج وحذف المحادثات وتصدير البيانات.

بيئات المؤسسات

توفر الحلول المؤسسية عادةً مستويات إضافية من الحماية وإدارة البيانات مقارنة بالحسابات الفردية.

الخصوصية وحماية البيانات فيClaude

نظرة عامة

Claudeهو نموذج ذكاء اصطناعي طورته شركة Anthropic ويركز على مفاهيم السلامة والموثوقية والحوكمة.

معالجة البيانات

يدعم: النصوص والملفات والتحليل الطويل للمستندات.

ميزات الخصوصية

تشمل: أدوات إدارة البيانات وسياسات مؤسسية وضوابط استخدام متقدمة.

الموصلات(Connectors)

قد تسمح بعض البيئات المؤسسية بربط Claude مع أنظمة خارجية وويستلزم ذلك إدارة دقيقة للصلاحيات والوصول إلى البيانات.

الخصوصية وحماية البيانات فيGemini

نظرة عامة

Geminiهو نموذج الذكاء الاصطناعي التوليدي المطور من قبل.Google

التكامل مع منظومةGoogle

قد يتكامل مع: البريد الإلكتروني والمستندات والتخزين السحابي وتطبيقات Google Workspace.

اعتبارات الخصوصية

ينبغي فهم: إعدادات النشاط وسياسات الاحتفاظ بالبيانات والصلاحيات الممنوحة للتطبيقات.

بيئات المؤسسات

توفر خدمات المؤسسات عادةً ضوابط إضافية لحماية البيانات وإدارة الوصول.

الخصوصية وحماية البيانات فيMicrosoft Copilot

نظرة عامة

Copilotهو مساعد ذكاء اصطناعي متكامل ضمن منظومة.Microsoft

مصادر البيانات

قد يتعامل مع: البريد الإلكتروني والملفات والاجتماعات والمستندات المؤسسية.

حماية البيانات

تعتمد مستويات الحماية بشكل كبير على: إعدادات Microsoft 365 وسياسات المؤسسة وإدارة الهوية والصلاحيات.

الميزة المؤسسية

يستفيد Copilot من ضوابط الأمان والامتثال الموجودة ضمن بيئة.Microsoft 365

المخاطر العملية عند استخدام أدوات الذكاء الاصطناعي

إدخال بيانات سرية

من أكثر الأخطاء شيوعاً: إدخال كلمات المرور ومفاتيح API والبيانات المالية وبيانات العملاء.

رفع مستندات حساسة

مثل: العقود السرية والتقارير الداخلية وقواعد البيانات.

مشاركة البيانات دون قصد

قد يشارك الموظفون معلومات حساسة أثناء طلب المساعدة أو التحليل.

سوء فهم سياسات الخدمة

عدم قراءة شروط الاستخدام وسياسات الخصوصية قد يؤدي إلى استخدام غير آمن للمنصة.

البيانات التي يجب عدم إدخالها

ينبغي تجنب إدخال: البيانات الصحية مثل: التشخيصات الطبية والسجلات العلاجية والبيانات المالية مثل: أرقام الحسابات والبطاقات البنكية وبيانات الهوية مثل: الرقم الوطني وجواز السفر والأسرار التجارية مثل: خطط الأعمال والأكواد السرية والأسرار الصناعية وبيانات العملاء خصوصاً إذا كانت تحتوي على معلومات شخصية.

أفضل الممارسات للأفراد

إزالة المعلومات الحساسة

استخدام بيانات مجهولة أو مستعارة عند الإمكان.

مراجعة النتائج

عدم الاعتماد الكامل على مخرجات الذكاء الاصطناعي.

استخدام المصادقة متعددة العوامل

لحماية الحسابات من الاختراق.

مراجعة إعدادات الخصوصية

بشكل دوري.

حذف المحادثات غير الضرورية

لتقليل كمية البيانات المخزنة.

أفضل الممارسات للمؤسسات

وضع سياسة استخدام واضحة

تحدد: المسموح والممنوع والبيانات الحساسة.

تدريب الموظفين

رفع مستوى الوعي بالمخاطر.

تصنيف البيانات

قبل استخدامها في الأنظمة الذكية.

استخدام الحلول المؤسسية

عند التعامل مع بيانات حساسة.

إجراء تقييم مخاطر

قبل اعتماد أي منصة جديدة.

مقارنة بين ChatGPT و Claudeو Geminiو Copilot

العنصر	ChatGPT	Claude	Gemini	Copilot
النصوص	ممتاز	ممتاز	ممتاز	ممتاز

العنصر	ChatGPT	Claude	Gemini	Copilot
تحليل الملفات	متقدم	متقدم	متقدم	متقدم
التكامل المؤسسي	مرتفع	مرتفع	مرتفع	مرتفع جداً
التكامل مع البريد	محدود	محدود	قوي	قوي جداً
بيئات العمل المؤسسية	متقدمة	متقدمة	متقدمة	متقدمة جداً
إدارة الخصوصية	متاحة	متاحة	متاحة	متاحة

الذكاء الاصطناعي التوليدي والامتثال

عند استخدام هذه الأدوات يجب مراعاة:

- GDPR
- قانون حماية البيانات الأردني
- PDPLالسعودي
- سياسات المؤسسة
- متطلبات الأمن السيبراني

ولا ينبغي اعتبار الذكاء الاصطناعي بديلاً عن الضوابط القانونية والتنظيمية.

مستقبل الخصوصية في أدوات الذكاء الاصطناعي

من المتوقع خلال السنوات القادمة: زيادة الشفافية وتحسين أدوات التحكم بالبيانات وتوسع الحلول المحلية (On-Premise) وتعزيز الامتثال التنظيمي وظهور معايير عالمية موحدة.

كما ستزداد أهمية النماذج المحلية المستضافة داخل المؤسسات لتقليل المخاطر المرتبطة بالبيانات الحساسة.

خاتمة الفصل

أصبحت أدوات الذكاء الاصطناعي التوليدي جزءاً أساسياً من بيئات العمل الحديثة، إلا أن استخدامها يتطلب فهماً عميقاً للجوانب المتعلقة بالخصوصية وحماية البيانات. وتختلف المنصات في خصائصها وسياساتها وإعداداتها، لكن المسؤولية النهائية عن حماية البيانات تبقى مشتركة بين مزود الخدمة والمؤسسة والمستخدم.

ويُعد تطبيق أفضل الممارسات والالتزام بالسياسات القانونية والتنظيمية شرطاً أساسياً للاستفادة من قدرات هذه الأدوات دون تعريض البيانات أو الحقوق الرقمية للخطر.

الفصل الثامن عشر: النماذج المحلية للذكاء الاصطناعي **(Local AI Models)** وحماية البيانات

مقدمة الفصل

مع التوسع المتزايد في استخدام الذكاء الاصطناعي داخل المؤسسات، أصبحت مسألة حماية البيانات والسيادة الرقمية من أهم التحديات التي تواجه صناع القرار ومديري تقنية المعلومات. فعلى الرغم من المزايا الكبيرة التي توفرها الخدمات السحابية للذكاء الاصطناعي، فإن العديد من المؤسسات الحكومية والمالية والصحية لا تستطيع إرسال بياناتها الحساسة إلى مزودي الخدمات الخارجيين بسبب المتطلبات القانونية أو الأمنية أو التنظيمية.

وقد أدى ذلك إلى ظهور توجه متزايد نحو استخدام النماذج المحلية(Local AI Models) ، والتي يتم تشغيلها داخل البنية التحتية الخاصة بالمؤسسة دون الحاجة إلى إرسال البيانات إلى خوادم خارجية.

ويكتسب هذا الاتجاه أهمية خاصة في ظل تصاعد المخاوف المتعلقة بالخصوصية، والامتثال التنظيمي، والسيادة الرقمية، وحماية الأسرار التجارية.

يهدف هذا الفصل إلى دراسة مفهوم النماذج المحلية، وأبرز المنصات المستخدمة لتشغيلها، والمزايا والتحديات المرتبطة بها، ودورها في تعزيز حماية البيانات داخل المؤسسات.

تعريف النماذج المحلية

نماذج الذكاء الاصطناعي التي يتم تشغيلها ومعالجتها داخل البنية التحتية الخاصة بالمؤسسة أو على أجهزة المستخدمين دون الاعتماد على مزود خدمة سحابي خارجي.

الفرق بين النماذج السحابية والمحلية

النماذج المحلية	النماذج السحابية	العنصر
داخل المؤسسة	خوادم خارجية	مكان المعالجة
عالية	محدودة نسبياً	السيطرة على البيانات
ليست ضرورية	غالباً مطلوبة	الحاجة للإنترنت
أسهل	أكثر تعقيداً	الامتثال التنظيمي

العنصر	النماذج السحابية	النماذج المحلية
التكلفة الأولية	منخفضة	أعلى
المرونة	مرتفعة	مرتفعة

أسباب التوجه نحو النماذج المحلية

تشمل: حماية البيانات الحساسة والامتثال للقوانين وتقليل الاعتماد على الأطراف الخارجية وتحسين السيطرة على البنية التحتية وتقليل مخاطر نقل البيانات عبر الحدود.

المنصات المحلية الشهيرة

Ollama

التعريف

Ollamaمنصة مفتوحة المصدر تسهل تشغيل نماذج الذكاء الاصطناعي محلياً.

المزايا سهولة التثبيت ودعم Windows وLinux وmacOS وإدارة بسيطة للنماذج ودعم العديد من النماذج الحديثة.

الاستخدامات المساعدات الذكية وتحليل المستندات والبرمجة وتطبيقات المؤسسات.

LM Studio

التعريف بيئة رسومية لتشغيل النماذج المحلية دون الحاجة إلى خبرة تقنية متقدمة والمزايا واجهة سهلة الاستخدام ودعم واسع للنماذج ومناسب للمستخدمين غير المتخصصين.

vLLM

التعريف منصة متقدمة مخصصة لتشغيل النماذج الكبيرة بكفاءة عالية والمزايا أداء مرتفع وإدارة فعالة للذاكرة ودعم البيئات المؤسسية.

الاستخدامات الأنظمة الإنتاجية ومراكز البيانات وتطبيقات الذكاء الاصطناعي واسعة النطاق.

llama.cpp

التعريف مشروع مفتوح المصدر يسمح بتشغيل النماذج على أجهزة ذات موارد محدودة والمزايا استهلاك منخفض للموارد ودعم المعالجات التقليدية وسهولة التخصيص.

النماذج المفتوحة الشائعة

Llama

طورتها شركة Meta وتعد من أكثر النماذج المفتوحة انتشاراً.

Qwen

طورتها Alibaba وتتميز بأداء قوي في: اللغة العربية والبرمجة والاستدلال المنطقي.

Mistral

تركز على الكفاءة والأداء وتستخدم على نطاق واسع في البيئات المؤسسية.

Gemma

طورتها Google وتوفر نماذج خفيفة نسبياً للاستخدام المحلي.

DeepSeek

أصبحت من أبرز النماذج المستخدمة في مهام البرمجة والاستدلال.

مزايا النماذج المحلية في حماية البيانات

السيادة الكاملة على البيانات

تبقى البيانات داخل المؤسسة طوال دورة حياتها.

تقليل مخاطر التسريب

عدم إرسال البيانات إلى مزود خارجي يقلل مساحة التعرض للمخاطر.

الامتثال التنظيمي

يساعد على الامتثال لـ:

- GDPR
- قانون حماية البيانات الأردني
- PDPLالسعودي
- السياسات الداخلية

التحكم الكامل

يمكن للمؤسسة: تحديد الصلاحيات ومراقبة الاستخدام وتطبيق سياسات الأمان الخاصة بها.

التحديات المرتبطة بالنماذج المحلية

التكلفة

تشمل: الخوادم ووحدات معالجة الرسومات (GPU) والصيانة.

إدارة البنية التحتية

تحتاج إلى: خبرات تقنية وتحديثات مستمرة ومراقبة الأداء.

تحديث النماذج

تتحمل المؤسسة مسؤولية: تنزيل التحديثات واختبارها ونشرها.

الأمن الداخلي

وجود النموذج داخل المؤسسة لا يعني غياب المخاطر وفقد تحدث: إساءة استخدام داخلية وأخطاء إعداد وتسريبات من الموظفين.

الأمن السيبراني للنماذج المحلية

6.1التحكم بالوصول

يجب تطبيق: إدارة الهوية والمصادقة متعددة العوامل ومبدأ أقل الصلاحيات.

التشفير

حماية: البيانات المخزنة والبيانات المنقولة والنسخ الاحتياطية.

مراقبة الأنشطة

تسجيل: المستخدمين والاستعلامات والعمليات الحساسة.

إدارة السجلات

ينبغي الاحتفاظ بسجلات تدقيق مناسبة لدعم الامتثال والتحقيقات.

إدارة البيانات الحساسة

البيانات الصحية

تتطلب: تشفيراً قوياً ورقابة صارمة وسجلات تدقيق.

البيانات المالية

تحتاج إلى ضوابط إضافية لحماية العملاء والمعاملات.

البيانات الحكومية

تخضع غالباً لمتطلبات سيادة البيانات والأمن الوطني.

الأسرار التجارية

يجب منع استخدامها في نماذج عامة أو بيئات غير خاضعة للرقابة.

النماذج المحلية في القطاعات المختلفة

القطاع الحكومي تساعد على: حماية بيانات المواطنين وتعزيز السيادة الرقمية وتقليل الاعتماد على مزودي الخدمات الأجانب.

القطاع المالي تستخدم في: تحليل المخاطر وخدمة العملاء واكتشاف الاحتيال ومع الحفاظ على سرية البيانات.

القطاع الصحي تمكن من استخدام الذكاء الاصطناعي دون تعريض السجلات الطبية للخطر والقطاع التعليمي تسمح ببناء مساعدين تعليميين محليين مع حماية بيانات الطلبة.

بناء بيئة ذكاء اصطناعي آمنة داخل المؤسسة

المرحلة الأولى: التخطيط

تحديد: الأهداف وأنواع البيانات والمتطلبات القانونية.

المرحلة الثانية: اختيار النموذج

اختيار النموذج المناسب وفق: الأداء واللغة والتكلفة وحجم البيانات.

المرحلة الثالثة: البنية التحتية

تشمل: الخوادم والشبكات والتخزين والنسخ الاحتياطي.

المرحلة الرابعة: الحوكمة

وضع: السياسات والضوابط وآليات المراجعة.

المرحلة الخامسة: التشغيل والمراقبة

متابعة: الأداء والامتثال والحوادث الأمنية.

الذكاء الاصطناعي المحلي والسيادة الرقمية

مفهوم السيادة الرقمية

تشير السيادة الرقمية إلى قدرة الدولة أو المؤسسة على التحكم في بياناتها وتقنياتها وبنيتها التحتية الرقمية.

دور النماذج المحلية

تسهم في: حماية البيانات الوطنية وتقليل التبعية التقنية وتعزيز الأمن المعلوماتي.

الاتجاهات العالمية

تتجه العديد من الدول والمؤسسات الكبرى نحو: النماذج المحلية والسحب السيادية والذكاء الاصطناعي الوطني.

مستقبل النماذج المحلية

من المتوقع خلال السنوات القادمة: تحسن أداء النماذج المفتوحة وانخفاض متطلبات التشغيل وزيادة الاعتماد المؤسسي وظهور حلول هجينة تجمع بين المحلي والسحابي وتوسع استخدام الذكاء الاصطناعي داخل المؤسسات الحساسة.

خاتمة الفصل

تمثل النماذج المحلية للذكاء الاصطناعي خياراً استراتيجياً للمؤسسات التي تتعامل مع بيانات حساسة أو تخضع لمتطلبات تنظيمية صارمة. فهي توفر مستوى أعلى من السيطرة والخصوصية والسيادة الرقمية مقارنة بالنماذج السحابية، وإن كانت تتطلب استثمارات وخبرات إضافية في البنية التحتية والأمن والإدارة.

ومع استمرار تطور النماذج المفتوحة المصدر وتحسن أدائها، يتوقع أن تصبح النماذج المحلية جزءاً أساسياً من استراتيجيات الذكاء الاصطناعي المؤسسية خلال السنوات القادمة.

الفصل التاسع عشر: الخصوصية وحماية البيانات في الحوسبة السحابية

مقدمة الفصل

أصبحت الحوسبة السحابية (Cloud Computing) إحدى أهم التقنيات التي تعتمد عليها المؤسسات الحديثة في تشغيل التطبيقات وتخزين البيانات وإدارة البنية التحتية الرقمية. فقد ساهمت الخدمات السحابية في خفض التكاليف التشغيلية وزيادة المرونة وسرعة التوسع، مما جعلها الخيار المفضل للعديد من المؤسسات الحكومية والخاصة على مستوى العالم.

إلا أن نقل البيانات إلى البيئات السحابية يثير مجموعة من التحديات المتعلقة بالخصوصية وحماية البيانات والأمن السيبراني والامتثال القانوني، خصوصاً عندما تتضمن البيانات معلومات شخصية أو حساسة أو عندما يتم تخزينها في مراكز بيانات تقع خارج حدود الدولة.

وتزداد أهمية هذه القضايا في عصر الذكاء الاصطناعي، حيث تعتمد العديد من الأنظمة الذكية على البنية السحابية لتوفير قدرات المعالجة والتخزين واسعة النطاق.

يهدف هذا الفصل إلى دراسة العلاقة بين الحوسبة السحابية وحماية البيانات الشخصية، وتحليل المخاطر والتحديات المرتبطة بها، واستعراض أفضل الممارسات لضمان الاستخدام الآمن والمتوافق مع المتطلبات القانونية.

تعريف الحوسبة السحابية

نموذج لتوفير الموارد الحاسوبية عند الطلب عبر الإنترنت، بما يشمل الخوادم والتخزين وقواعد البيانات والشبكات والبرمجيات والخدمات المختلفة.

خصائص الحوسبة السحابية

الخدمة الذاتية إمكانية الحصول على الموارد دون تدخل بشري مباشر من المزود والوصول الواسع الوصول إلى الخدمات من أي مكان عبر الإنترنت وتجميع الموارد مشاركة الموارد بين عدد كبير من المستخدمين والمرونة والتوسع إمكانية زيادة أو تقليل الموارد حسب الحاجة والدفع حسب الاستخدام دفع التكاليف بناءً على الاستهلاك الفعلي.

نماذج الخدمات السحابية

البنية التحتية كخدمة(IaaS)

يوفر المزود: الخوادم والشبكات والتخزين وبينما تدير المؤسسة: التطبيقات والبيانات وأنظمة التشغيل.

أمثلة

- Amazon EC2
- Microsoft Azure Virtual Machines
- Google Compute Engine

المنصة كخدمة(PaaS)

توفر بيئة متكاملة لتطوير وتشغيل التطبيقات.

أمثلة

- Azure App Service
- Google App Engine
- Heroku

البرمجيات كخدمة(SaaS)

يستخدم العميل التطبيق مباشرة دون إدارة البنية التحتية.

أمثلة

- Microsoft 365
- Google Workspace
- Salesforce

نماذج النشر السحابي

السحابة العامة

يتم تشغيلها بواسطة مزود خدمة خارجي وتُستخدم من قبل عدة عملاء.

السحابة الخاصة

تخصص لمؤسسة واحدة فقط.

السحابة الهجينة

تجمع بين السحابة العامة والخاصة.

السحابة السيادية

مصممة لتلبية متطلبات السيادة الرقمية والقوانين المحلية.

البيانات الشخصية في البيئة السحابية

طبيعة البيانات المخزنة

قد تتضمن البيئات السحابية: بيانات العملاء والسجلات الصحية والبيانات المالية وبيانات الموظفين والوثائق القانونية.

دورة حياة البيانات السحابية

تمر البيانات بالمراحل التالية: الجمع والنقل والتخزين والمعالجة والأرشفة والحذف وويجب حماية البيانات في كل مرحلة.

مخاطر الخصوصية في الحوسبة السحابية

فقدان السيطرة المباشرة

عند تخزين البيانات لدى مزود خارجي تقل السيطرة المباشرة للمؤسسة على البنية التحتية.

الوصول غير المصرح به

قد تنشأ المخاطر بسبب: أخطاء إعداد وسرقة الحسابات وضعف الصلاحيات.

تعدد المستأجرين

تعتمد السحابات العامة غالباً على بيئة مشتركة بين عدة عملاء ومما يفرض تحديات إضافية تتعلق بالعزل الأمني.

الاحتفاظ المفرط بالبيانات

قد يتم الاحتفاظ بالبيانات لفترات أطول من المطلوب قانونياً.

إساءة استخدام البيانات

من المخاطر المحتملة: الاستخدام غير المصرح به ومشاركة البيانات مع أطراف ثالثة دون أساس قانوني.

نقل البيانات عبر الحدود

مفهوم النقل الدولي

يحدث عندما يتم تخزين البيانات أو معالجتها في دولة أخرى.

التحديات القانونية

تشمل: اختلاف مستويات الحماية القانونية واختلاف السلطات القضائية وصعوبة إنفاذ الحقوق.

المتطلبات القانونية

تتطلب معظم التشريعات: ضمانات قانونية وعقود مناسبة ومستوى حماية مكافئ.

نموذج المسؤولية المشتركة

يُعد نموذج المسؤولية المشتركة أحد أهم مفاهيم الأمن السحابي.

مسؤوليات مزود الخدمة

تشمل: مراكز البيانات والأجهزة والشبكات والبنية التحتية الأساسية.

مسؤوليات العميل

تشمل: البيانات والمستخدمين والصلاحيات وإعدادات الأمان والامتثال التنظيمي.

سوء الفهم الشائع

يعتقد بعض العملاء أن مزود الخدمة مسؤول عن كل شيء، وهو اعتقاد غير صحيح.

التشفير وإدارة المفاتيح

أهمية التشفير

يُعد التشفير من أهم وسائل حماية البيانات السحابية.

التشفير أثناء النقل

يحمي البيانات أثناء انتقالها عبر الشبكات.

التشفير أثناء التخزين

يحمي البيانات داخل الخوادم وقواعد البيانات.

إدارة المفاتيح

تعد إدارة مفاتيح التشفير من أهم عناصر الأمن السحابي وويجب: حماية المفاتيح وتدويرها دورياً وتقييد الوصول إليها.

إدارة الهوية والوصول

إدارة الهوية

تضمن التحقق من هوية المستخدمين.

المصادقة متعددة العوامل

تضيف طبقة إضافية من الحماية.

مبدأ أقل الصلاحيات

منح المستخدمين الحد الأدنى اللازم من الصلاحيات.

المراجعة الدورية

فحص الصلاحيات وإزالة الحسابات غير المستخدمة.

الامتثال القانوني في البيئات السحابية

الامتثال لـ GDPR

يجب التأكد من: قانونية المعالجة ونقل البيانات بشكل مشروع واحترام حقوق الأفراد.

الامتثال للقانون الأردني

يتطلب الالتزام بأحكام حماية البيانات الشخصية داخل المملكة.

الامتثال لـ PDPL السعودي

يفرض متطلبات خاصة على معالجة البيانات ونقلها.

الامتثال القطاعي

قد تخضع بعض القطاعات لمتطلبات إضافية مثل: الصحة والبنوك والاتصالات.

الأمن السيبراني في البيئات السحابية

المراقبة المستمرة

متابعة الأنشطة والتهديدات بشكل دائم.

النسخ الاحتياطي

إنشاء نسخ احتياطية منتظمة ومحمية.

اكتشاف التهديدات

استخدام أدوات تحليل السجلات والكشف المبكر.

إدارة الثغرات

تحديث الأنظمة وإصلاح نقاط الضعف باستمرار.

الذكاء الاصطناعي والحوسبة السحابية

تعتمد معظم خدمات الذكاء الاصطناعي الحديثة على البنية السحابية.

ومن أبرز الاستخدامات: تدريب النماذج والاستدلال (Inference) وتحليل البيانات وخدمات الذكاء الاصطناعي التوليدي.

التحديات

تشمل: نقل البيانات الحساسة والامتثال القانوني والشفافية وإدارة المخاطر.

أفضل الممارسات لحماية البيانات في السحابة

ينبغي على المؤسسات: تصنيف البيانات قبل نقلها للسحابة وتطبيق التشفير الشامل وتفعيل المصادقة متعددة العوامل ومراجعة الصلاحيات دورياً وإجراء تقييمات مخاطر منتظمة وفهم نموذج المسؤولية المشتركة ومراجعة العقود مع مزودي الخدمات ومراقبة الامتثال القانوني وإعداد خطط استجابة للحوادث وتنفيذ اختبارات أمنية دورية.

مستقبل الخصوصية في الحوسبة السحابية

من المتوقع خلال السنوات القادمة: توسع السحب السيادية وزيادة متطلبات الامتثال ودمج الذكاء الاصطناعي في إدارة الأمن وتطور تقنيات التشفير وزيادة الاعتماد على الحوسبة السرية (Confidential Computing).

كما ستصبح حماية البيانات أحد المعايير الأساسية عند اختيار مزود الخدمة السحابية.

خاتمة الفصل

تمثل الحوسبة السحابية حجر الأساس للبنية الرقمية الحديثة، إلا أن استخدامها يفرض مسؤوليات إضافية تتعلق بحماية البيانات والخصوصية والامتثال القانوني. وتحتاج المؤسسات إلى فهم واضح للمخاطر والضوابط المرتبطة بالبيئات السحابية، وتطبيق ممارسات أمنية وقانونية مناسبة لضمان الاستفادة من مزايا السحابة دون تعريض البيانات للخطر.

ومع استمرار تطور الخدمات السحابية والذكاء الاصطناعي، ستصبح إدارة الخصوصية والأمن في السحابة أحد أهم عناصر الحوكمة الرقمية المؤسسية.

الفصل العشرون: إدارة الحوادث واختراقات البيانات الشخصية

مقدمة الفصل

في ظل التوسع المتسارع في استخدام الأنظمة الرقمية والحوسبة السحابية والذكاء الاصطناعي، أصبحت حوادث البيانات واختراقات الأمن السيبراني من أبرز التحديات التي تواجه المؤسسات حول العالم. وتشير الدراسات الدولية إلى أن احتمالية تعرض أي مؤسسة لحادث أمني أصبحت مسألة وقت أكثر من كونها احتمالاً بعيداً، مما يجعل الاستعداد المسبق والاستجابة الفعالة ضرورة استراتيجية لا غنى عنها.

ولا يقتصر أثر حوادث البيانات على الجوانب التقنية فقط، بل يمتد إلى الجوانب القانونية والمالية والتشغيلية والسمعة المؤسسية. فقد يؤدي اختراق بسيط إلى تسريب بيانات آلاف العملاء أو تعطيل خدمات حيوية أو فرض غرامات تنظيمية كبيرة.

ولهذا السبب أصبحت إدارة الحوادث الأمنية جزءاً أساسياً من برامج حماية البيانات والحوكمة المؤسسية والأمن السيبراني.

يهدف هذا الفصل إلى دراسة مفهوم حوادث البيانات الشخصية وأنواعها وآليات اكتشافها والاستجابة لها والتحقيق فيها والإبلاغ عنها، بالإضافة إلى استعراض أفضل الممارسات لبناء برنامج متكامل لإدارة الحوادث.

مفهوم حادث البيانات الشخصية

تعريف حادث البيانات

يقصد بحادث البيانات الشخصية:

أي حدث يؤدي بصورة عرضية أو غير مشروعة إلى تدمير البيانات الشخصية أو فقدانها أو تعديلها أو الكشف عنها أو الوصول إليها دون تصريح.

الفرق بين الحادث الأمني واختراق البيانات

الحادث الأمني أي حدث يؤثر على أمن المعلومات.

اختراق البيانات نوع خاص من الحوادث يؤدي إلى: كشف البيانات وسرقتها والوصول غير المصرح به إليها.

أهمية التعامل السريع

كلما تم اكتشاف الحادث والاستجابة له بسرعة: انخفض حجم الضرر وقلت الخسائر وتحسن الامتثال القانوني.

أنواع حوادث البيانات الشخصية

فقدان السرية

عندما تصبح البيانات متاحة لأشخاص غير مصرح لهم وأمثلة تسريب قاعدة بيانات وإرسال معلومات لجهة خاطئة واختراق حسابات المستخدمين.

فقدان السلامة

عندما يتم تعديل البيانات بصورة غير مصرح بها وأمثلة تغيير السجلات والتلاعب بالبيانات المالية وتعديل البيانات الطبية.

فقدان التوافر

عندما تصبح البيانات أو الأنظمة غير متاحة وأمثلة هجمات الفدية وتعطل الخوادم وحذف الملفات.

أسباب حوادث البيانات

الأخطاء البشرية

تُعد من أكثر الأسباب شيوعاً وأمثلة إرسال بريد إلكتروني بالخطأ ومشاركة ملفات حساسة وإعدادات أمنية غير صحيحة.

الهجمات الإلكترونية

تشمل: التصيد الإلكتروني والبرمجيات الخبيثة وهجمات الفدية واستغلال الثغرات.

التهديدات الداخلية

قد تصدر من: موظفين ومتعاقدين وشركاء أعمال.

الأعطال التقنية

مثل: فشل الأجهزة وأخطاء البرمجيات وفقدان النسخ الاحتياطية.

اكتشاف الحوادث الأمنية

أهمية الاكتشاف المبكر

كل دقيقة تأخير قد تزيد من: حجم الاختراق وعدد المتضررين والخسائر المالية.

مؤشرات الاختراق

نشاط غير طبيعي مثل تسجيل دخول من مواقع غير معتادة ونقل بيانات بكميات كبيرة خصوصاً خارج أوقات العمل وتغييرات غير مبررة في الحسابات أو الأنظمة وتنبيهات أنظمة الحماية الصادرة عن أدوات المراقبة.

مصادر الاكتشاف

أنظمة SIEM وأنظمة كشف التسلل وفرق الأمن السيبراني وبلاغات الموظفين وبلاغات العملاء.

دورة الاستجابة للحوادث

تعتمد معظم الأطر العالمية على دورة متكاملة للاستجابة للحوادث.

المرحلة الأولى: التحضير

تشمل: تشكيل فريق الاستجابة وإعداد السياسات وتوفير الأدوات والتدريب المستمر.

المرحلة الثانية: الاكتشاف والتحليل

تحديد: نوع الحادث ونطاقه وتأثيره.

المرحلة الثالثة: الاحتواء

منع انتشار الحادث وأمثلة عزل الخادم وتعطيل الحسابات وإيقاف الخدمات المتأثرة.

المرحلة الرابعة: المعالجة

إزالة السبب الجذري للحادث ومثل: إزالة البرمجيات الخبيثة وإصلاح الثغرات وتغيير كلمات المرور.

المرحلة الخامسة: التعافي

استعادة: الأنظمة والخدمات والبيانات وإلى وضع التشغيل الطبيعي.

المرحلة السادسة: المراجعة

تحليل:

- ما الذي حدث؟
- لماذا حدث؟
- كيف يمكن منع تكراره؟

فريق الاستجابة للحوادث

مفهوم الفريق

هو مجموعة من المختصين المسؤولين عن إدارة الحوادث الأمنية.

التخصصات المطلوبة

الأمن السيبراني تحليل الحادث واحتواؤه وتقنية المعلومات استعادة الأنظمة والشؤون القانونية تحليل الالتزامات القانونية وحماية البيانات تقييم تأثير الحادث على الأفراد والعلاقات العامة إدارة الاتصالات الإعلامية.

مفهوم التحقيق الجنائي الرقمي

هو عملية جمع وتحليل الأدلة الرقمية بطريقة قانونية ومنهجية.

أهداف التحقيق

تحديد مصدر الهجوم ومعرفة كيفية حدوثه وجمع الأدلة ودعم الإجراءات القانونية.

الأدلة الرقمية

تشمل: سجلات الأنظمة ورسائل البريد الإلكتروني والملفات وبيانات الشبكات.

سلسلة حفظ الأدلة

يجب الحفاظ على الأدلة دون تعديل لضمان قبولها قانونياً.

تقييم أثر الحادث

تحديد البيانات المتأثرة

ما نوع البيانات التي تعرضت للحادث؟

عدد الأفراد المتضررين

كم عدد الأشخاص المتأثرين؟

مستوى الحساسية

هل تشمل البيانات:

- صحية؟
- مالية؟
- بيومترية؟

- حكومية؟

احتمالية الضرر

ما احتمال تعرض الأفراد لأضرار نتيجة الحادث؟

الإبلاغ عن الحوادث

أهمية الإبلاغ

يعد الإبلاغ أحد أهم متطلبات الامتثال القانوني.

الجهات الرقابية

قد تشمل: هيئات حماية البيانات والجهات التنظيمية والجهات القضائية وهيئات الأمن السيبراني.

محتوى الإبلاغ

يتضمن عادة: وصف الحادث ونوع البيانات المتأثرة وعدد الأفراد المتضررين والإجراءات المتخذة.

التواصل مع أصحاب البيانات

متى يجب الإبلاغ؟

عندما يشكل الحادث خطراً على حقوق الأفراد أو حرياتهم.

أهداف التواصل

الشفافية وتقليل الضرر وتمكين الأفراد من اتخاذ الاحتياطات اللازمة.

محتوى الإشعار

ينبغي أن يتضمن: طبيعة الحادث والبيانات المتأثرة والمخاطر المحتملة والإجراءات الوقائية المقترحة.

بناء خطة استجابة لحوادث البيانات

أهداف الخطة

تقليل الأضرار وتسريع الاستجابة وضمان الامتثال وحماية السمعة.

عناصر الخطة

نطاق التطبيق ما الحوادث التي تغطيها الخطة؟

المسؤوليات من المسؤول عن ماذا؟

إجراءات الاستجابة خطوات واضحة ومحددة.

آليات التصعيد متى يتم إشراك الإدارة العليا؟

قنوات الاتصال الداخلية والخارجية والمراجعة الدورية تحديث الخطة باستمرار.

العلاقة بين حوادث البيانات والقوانين

تفرض العديد من التشريعات متطلبات محددة للتعامل مع الحوادث وGDPR الإبلاغ خلال مدد قانونية محددة.

القانون الأردني يفرض التزامات مرتبطة بحماية البيانات والإبلاغ وفق الأحكام التنظيمية المعمول بها.

PDPLالسعودي يتطلب إجراءات واضحة للإبلاغ والتعامل مع الحوادث.

دور الذكاء الاصطناعي في إدارة الحوادث

يمكن استخدام الذكاء الاصطناعي في: اكتشاف الهجمات وتحليل السجلات وتحديد الأنماط المشبوهة وتسريع الاستجابة.

المخاطر المرتبطة

قد يستخدم المهاجمون الذكاء الاصطناعي أيضاً في: أتمتة الهجمات والتصيد المتقدم وتجاوز بعض الضوابط الأمنية.

أفضل الممارسات المؤسسية

ينبغي على المؤسسات: إنشاء فريق استجابة متخصص وإعداد خطة مكتوبة ومحدثة وتنفيذ تدريبات دورية ومراقبة الأنظمة باستمرار والاحتفاظ بسجلات دقيقة وحماية الأدلة الرقمية وتقييم الحوادث بانتظام ومراجعة الدروس المستفادة ودمج إدارة الحوادث ضمن الحوكمة المؤسسية وتعزيز ثقافة الأمن والخصوصية.

خاتمة الفصل

تمثل حوادث البيانات الشخصية أحد أخطر التحديات التي تواجه المؤسسات في العصر الرقمي، نظراً لما قد يترتب عليها من آثار قانونية ومالية وتشغيلية وسمعة سلبية. ولذلك لم يعد التركيز مقتصراً على منع الحوادث فقط، بل أصبح يشمل القدرة على اكتشافها والاستجابة لها والتعافي منها بصورة فعالة ومنظمة.

ويُعد وجود خطة استجابة متكاملة وفريق مؤهل وثقافة مؤسسية واعية من أهم عوامل النجاح في إدارة حوادث البيانات وتقليل آثارها السلبية.

الملاحق

الملحق الأول: معجم المصطلحات

أ

الأمن السيبراني(Cybersecurity)

مجموعة السياسات والإجراءات والتقنيات المستخدمة لحماية الأنظمة والشبكات والبيانات من الهجمات والاختراقات الإلكترونية.

الأثر الأخلاقي للذكاء الاصطناعي(AI Ethical Impact)

النتائج والتبعات الأخلاقية الناتجة عن استخدام أنظمة الذكاء الاصطناعي على الأفراد والمجتمعات.

ب

البيانات(Data)

مجموعة الحقائق أو المعلومات الخام التي يمكن تخزينها أو معالجتها أو تحليلها.

البيانات الشخصية(Personal Data)

أي معلومات تتعلق بشخص طبيعي محدد أو يمكن التعرف عليه بصورة مباشرة أو غير مباشرة.

البيانات الحساسة(Sensitive Personal Data)

فئة من البيانات الشخصية تتطلب حماية إضافية بسبب طبيعتها الخاصة، مثل البيانات الصحية والبيومترية والجينية والدينية.

البيانات البيومترية(Biometric Data)

البيانات الناتجة عن الخصائص الجسدية أو السلوكية للأفراد مثل بصمة الإصبع أو بصمة الوجه أو بصمة العين.

البيانات الجينية(Genetic Data)

البيانات المتعلقة بالخصائص الوراثية للفرد.

البيانات الضخمة(Big Data)

مجموعات بيانات كبيرة ومعقدة يصعب معالجتها باستخدام الأدوات التقليدية.

ت

التحيز الخوارزمي(Algorithmic Bias)

ميل النظام الذكي إلى إنتاج نتائج غير عادلة نتيجة تحيز البيانات أو تصميم الخوارزمية.

التشفير(Encryption)

عملية تحويل البيانات إلى صيغة غير مفهومة إلا للأشخاص المصرح لهم.

التزييف العميق(Deepfake)

محتوى مرئي أو صوتي يتم إنشاؤه أو تعديله بواسطة الذكاء الاصطناعي ليبدو حقيقياً.

التعلم الآلي(Machine Learning)

فرع من الذكاء الاصطناعي يمكّن الأنظمة من التعلم من البيانات وتحسين أدائها دون برمجة مباشرة.

التعلم العميق(Deep Learning)

فرع متقدم من التعلم الآلي يعتمد على الشبكات العصبية متعددة الطبقات.

ح

الحوسبة السحابية(Cloud Computing)

نموذج لتوفير الموارد والخدمات الحاسوبية عبر الإنترنت عند الطلب.

حوكمة الذكاء الاصطناعي(AI Governance)

مجموعة السياسات والإجراءات التي تنظم تطوير واستخدام أنظمة الذكاء الاصطناعي.

خ

خرق البيانات(Data Breach)

حادث يؤدي إلى الوصول غير المصرح به أو الكشف أو فقدان البيانات الشخصية.

ذ

الذكاء الاصطناعي(Artificial Intelligence)

قدرة الأنظمة الحاسوبية على أداء مهام تتطلب عادةً ذكاءً بشرياً.

الذكاء الاصطناعي التوليدي(Generative AI)

أنظمة ذكاء اصطناعي قادرة على إنشاء نصوص أو صور أو أصوات أو محتوى جديد.

س

سجل المعالجة(Processing Record)

وثيقة توثق عمليات معالجة البيانات الشخصية داخل المؤسسة.

السيادة الرقمية(Digital Sovereignty)

قدرة الدولة أو المؤسسة على التحكم الكامل ببياناتها وبنيتها الرقمية.

ش

الشفافية(Transparency)

إمكانية فهم كيفية جمع البيانات واستخدامها ومعالجتها.

م

المعالجة(Processing)

أي عملية تتم على البيانات الشخصية مثل الجمع أو التخزين أو التحليل أو الحذف.

المتحكم بالبيانات(Data Controller)

الشخص أو الجهة التي تحدد أغراض ووسائل معالجة البيانات الشخصية.

معالج البيانات(Data Processor)

الجهة التي تعالج البيانات نيابة عن المتحكم.

مسؤول حماية البيانات(DPO)

الشخص المسؤول عن متابعة الامتثال لقوانين حماية البيانات داخل المؤسسة.

نموذج اللغة الكبير(LLM)

نموذج ذكاء اصطناعي مدرب على كميات ضخمة من النصوص لفهم اللغة وتوليدها.

الملحق الثاني: قائمة الاختصارات

الاختصار	المعنى

المعنى	الاختصار
Artificial Intelligence	AI
Artificial General Intelligence	AGI
Large Language Model	LLM
Machine Learning	ML
Deep Learning	DL
Natural Language Processing	NLP
General Data Protection Regulation	GDPR
Personal Data Protection Law	PDPL
Data Protection Impact Assessment	DPIA
Data Protection Officer	DPO
AI Impact Assessment	AIA
International Organization for Standardization	ISO
National Institute of Standards and Technology	NIST
Confidentiality, Integrity, Availability	CIA

الاختصار	المعنى
SIEM	Security Information and Event Management
IDS	Intrusion Detection System
IPS	Intrusion Prevention System
MFA	Multi-Factor Authentication
API	Application Programming Interface
SaaS	Software as a Service
PaaS	Platform as a Service
IaaS	Infrastructure as a Service
RAG	Retrieval-Augmented Generation
SOC	Security Operations Center
CSIRT	Computer Security Incident Response Team

الملحق الثالث: نماذج قانونية

نموذج إشعار خصوصية

إشعار حماية البيانات الشخصية

تلتزم مؤسسة/شركة (اسم المؤسسة) بحماية البيانات الشخصية الخاصة بالمستخدمين وفقاً للتشريعات المعمول بها.

تشمل البيانات التي يتم جمعها:

- الاسم
- البريد الإلكتروني
- رقم الهاتف
- بيانات الحساب

أغراض المعالجة:

- تقديم الخدمات
- تحسين تجربة المستخدم
- الامتثال للالتزامات القانونية

حقوق صاحب البيانات:

- الوصول للبيانات
- التصحيح
- الحذف
- سحب الموافقة

للاستفسارات:

البريد الإلكتروني_____ :

نموذج موافقة على معالجة البيانات

أنا الموقع أدناه:

الاسم_____ :

أوافق على قيام_____

بجمع ومعالجة بياناتي الشخصية للأغراض التالية:

وأقر بأنني اطلعت على إشعار الخصوصية وفهمت حقوقي القانونية.

التوقيع_____ :

التاريخ_____ :

نموذج طلب وصول للبيانات

إلى: مسؤول حماية البيانات

أرغب بالحصول على نسخة من بياناتي الشخصية المخزنة لدى المؤسسة.

الاسم_____ :

رقم الهوية_____ :

البريد الإلكتروني_____ :

التوقيع_____ :

التاريخ_____ :

نموذج الإبلاغ عن حادث بيانات

رقم البلاغ_____ :

تاريخ الحادث_____ :

نوع الحادث:

□اختراق بيانات

□فقدان بيانات

□تعديل غير مشروع

□وصول غير مصرح به

وصف الحادث:

الإجراءات المتخذة:

اسم المبلغ:

الملحق الرابع: المراجع العربية

الكتب العربية

1. السالمي، علي .**أمن المعلومات والجرائم الإلكترونية** .دار الفكر الجامعي.
2. الخطيب، محمد .**حماية البيانات الشخصية في البيئة الرقمية** .دار الثقافة للنشر والتوزيع.

الشوابكة، محمد. القانون والجرائم الإلكترونية. دار وائل للنشر والزعبي، أحمد. الأمن السيبراني وإدارة المخاطر الرقمية. دار المسيرة.

3. عبد الحميد، طارق .**الذكاء الاصطناعي وتحديات القانون المعاصر** .المركز العربي للأبحاث.

التشريعات العربية

قانون حماية البيانات الشخصية الأردني رقم (24) لسنة 2023 ونظام حماية البيانات الشخصية السعودي (PDPL) وقانون حماية البيانات الشخصية الإماراتي الاتحادي وقانون حماية البيانات الشخصية البحريني وقانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020.

الملحق الخامس: المراجع الأجنبية

الكتب

1. Paul Voigt & Axel Von dem Bussche. *The EU General Data Protection Regulation (GDPR): A Practical Guide*. Springer.
2. Daniel J. Solove & Paul M. Schwartz. *Information Privacy Law*. Aspen Publishing.

Ronald Leenes et al. Data Protection and Privacy. Hart Publishing وKevin Warwick. Artificial Intelligence: The Basics. Routledge.

3. Stuart Russell & Peter Norvig. *Artificial Intelligence: A Modern Approach*. Pearson.

المعايير الدولية

ISO/IEC 27001 – Information Security Management Systems وISO/IEC 27701 – Privacy Information Management Systems وISO/IEC 42001 – Artificial Intelligence Management Systems وNIST Cybersecurity Framework (CSF)وNIST AI Risk Management Framework (AI RMF).

التشريعات الدولية

General Data Protection Regulation (GDPR) – European Union وEU Artificial Intelligence Act وCalifornia Consumer Privacy Act (CCPA) و California Privacy Rights Act (CPRA)وHealth Insurance Portability and Accountability Act (HIPAA) وChildren's Online Privacy Protection Act (COPPA).

خاتمة الكتاب

يمثل هذا الكتاب مرجعاً أكاديمياً وتطبيقياً يجمع بين مفاهيم حماية البيانات الشخصية، والأمن السيبراني، والذكاء الاصطناعي، والحوكمة، والامتثال القانوني. وقد تم إعداد محتواه ليخدم الباحثين والطلبة والمهنيين وصناع القرار، وليوفر فهماً متكاملاً للتحديات والفرص التي تفرضها الثورة الرقمية الحديثة.

إن حماية البيانات لم تعد مجرد متطلب قانوني أو تقني، بل أصبحت جزءاً من مسؤولية المؤسسات تجاه الأفراد والمجتمع، وعنصراً أساسياً في بناء الثقة الرقمية والتنمية المستدامة في عصر الذكاء الاصطناعي.

الدكتور زيد ربابعه