

ماجستير القانون الرقمي

جامعة ميدأوشن



إعداد

فهد حاسن الأحمدى

رقم الطالب : 253000565

**Research Methods For Law**

**Supervised By**

**Nourallah Elkolaly**

# المسؤولية القانونية عن انتهاك البيانات الشخصية في البيئة الرقمية

## دراسة مقارنة بين النظام السعودي والقانون المصري واللائحة الأوروبية (GDPR)

### فهرس البحث

#### المقدمة

1. الخلفية
2. مشكلة البحث
3. أهمية البحث
4. أهداف البحث
5. منهجية البحث

#### الباب الأول: الإطار المفاهيمي للبيانات الشخصية والخصوصية الرقمية

##### الفصل الأول: ماهية البيانات الشخصية في التشريعات المقارنة

1. المبحث الأول: التعريف التشريعي للبيانات الشخصية
  - المطلب الأول: التعريف في نظام حماية البيانات الشخصية السعودي
  - المطلب الثاني: التعريف في القانون المصري
  - المقارنة بين النظامين

##### 2. المبحث الثاني: أنواع البيانات الشخصية والتمييز بينها

- المطلب الأول: البيانات الشخصية العادية
- المطلب الثاني: البيانات الشخصية الحساسة (البيانات المحظورة)

##### الفصل الثاني: الطبيعة القانونية للبيانات الشخصية وخصائصها في البيئة الرقمية

1. المبحث الأول: الخصائص المميزة للبيانات الرقمية
2. المبحث الثاني: الطبيعة القانونية للحق في حماية البيانات

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

### . الفصل الأول: التزامات جهة التحكم ومعالجة البيانات

1. المبحث الأول: مبادئ المعالجة المشروعة

2. المبحث الثاني: الالتزامات التقنية والإدارية (أمن البيانات)

### . الفصل الثاني: حقوق صاحب البيانات وآليات ممارستها

1. المبحث الأول: الحق في العلم والوصول

2. المبحث الثاني: الحقوق التصحيحية والنهائية (الحق في النسيان)

## الباب الثالث: المسؤولية القانونية عن انتهاك البيانات الشخصية

### . الفصل الأول: أركان المسؤولية التقصيرية عن الانتهاك الرقمي

1. المبحث الأول: الخطأ في معالجة البيانات

2. المبحث الثاني: الضرر وعلاقة السببية في الفضاء الافتراضي

### . الفصل الثاني: الجزاءات المقررة وآليات جبر الضرر

1. المبحث الأول: المسؤولية الجنائية والعقوبات النظامية

2. المبحث الثاني: المسؤولية المدنية والتعويض

## الخاتمة والتوصيات

## المصادر والمراجع

# المسؤولية القانونية عن انتهاك البيانات الشخصية في البيئة الرقمية

## دراسة مقارنة بين النظام السعودي والقانون المصري واللائحة الأوروبية (GDPR)

### مقدمة البحث

تعد البيانات الشخصية في العصر الرقمي الركيزة الأساسية لكافة المعاملات الإلكترونية، حيث تجاوزت قيمتها الاقتصادية والاجتماعية الأصول المادية التقليدية. ومع تسارع التحول الرقمي في المملكة العربية السعودية وجمهورية مصر العربية، ظهرت تحديات قانونية كبيرة تتعلق بحماية هذه البيانات من الانتهاكات الرقمية، خاصة مع التطور التقني الذي جعل الاختراقات أسهل وأسرع وعابرة للحدود.

### مشكلة البحث

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

### أهمية البحث:

تكمن الأهمية في حداثة "نظام حماية البيانات الشخصية السعودي" والحاجة إلى تأصيل أحكامه مقارنة بالقانون المصري واللائحة الأوروبية GDPR، مما يساهم في تزويد الباحثين والقضاة بأطر عملية لمعالجة النزاعات التقنية المستحدثة.

### أهداف البحث:

1. توضيح المفهوم القانوني للبيانات الشخصية وأنواعها وحمايتها.
2. تحليل الالتزامات القانونية المترتبة على جهات التحكم والمعالجة.
3. دراسة حقوق صاحب البيانات وآليات ممارستها.
4. تفصيل المسؤولية القانونية المدنية والجنائية الناشئة عن الانتهاكات الرقمية.

### منهجية البحث:

يعتمد البحث على المنهج المقارن بين الأنظمة السعودية والمصرية واللائحة الأوروبية، إضافة إلى تحليل النصوص القانونية، والفقه القانوني، والدراسات الأكاديمية، وحالات الانتهاك الواقعية.

## الباب الأول: الإطار المفاهيمي للبيانات الشخصية

### الفصل الأول: ماهية البيانات الشخصية في التشريعات المقارنة

#### المبحث الأول: التعريف التشريعي للبيانات الشخصية

- **في النظام السعودي (٢٠٢١م):** المادة الأولى تحدد البيانات الشخصية بأنها كل بيان يؤدي إلى التعرف على الفرد مباشرة أو غير مباشرة، بما يشمل الاسم، رقم الهوية، العناوين، أرقام التواصل، الحسابات البنكية، البطاقات الائتمانية، الصور الثابتة والمتحركة، وغيرها.
- **التحليل:** المنهج واسع ويشمل جميع أشكال البيانات الرقمية وغير الرقمية. استخدام عبارة "بصفة مباشرة أو غير مباشرة" يشمل البيانات المشتقة من دمج بيانات أخرى.
- **في القانون المصري (١٥١ لسنة ٢٠٢٠):** يشمل أي بيانات متعلقة بشخص طبيعي يمكن تحديده مباشرة أو عبر الربط مع بيانات أخرى.
- **المقارنة:** كلا النظامين يستثنيان الأشخاص الاعتباريين ويقتصران على حماية الأشخاص الطبيعيين.

#### المبحث الثاني: أنواع البيانات الشخصية

1. **البيانات العادية:** الاسم، العنوان، رقم الهاتف، البريد الإلكتروني. معالجتها مشروطة بموافقة صريحة أو سند قانوني.
2. **البيانات الحساسة:** الأصل العرقي، المعتقدات الدينية، البيانات الجنائية، البيانات الحيوية والصحية. معالجة هذه البيانات مقيدة جداً، وانتهاكها يترتب عليه مسؤولية مدنية وجنائية صارمة.

#### التفصيل الموسع:

- **البيانات الحيوية:** بصمة الإصبع، بصمة الوجه، الحمض النووي، وهي فريدة وتبقى ثابتة مدى الحياة.
- **البيانات الصحية:** سجلات طبية وتشخيصات، لها قدسية خاصة في القانون السعودي والمصري.
- **أثر الانتهاك:** تسرب هذه البيانات قد يؤدي إلى أضرار دائمة للمواطن من الناحية المالية والنفسية.

## الفصل الثاني: الطبيعة القانونية للبيانات الشخصية وخصائصها

### المبحث الأول: الخصائص المميزة للبيانات الرقمية

1. **اللاتجسد:** البيانات غير ملموسة، مما يصعب حيازتها بالمعنى التقليدي.
2. **القابلية للنسخ واللامتناهي:** النسخ لا يحرم صاحب البيانات، لكن الضرر يكمن في اطلاع الغير.
3. **العبور عبر الحدود:** بيانات مواطن سعودي قد تعالج في خوادم خارجية، ما يثير إشكالية الاختصاص القضائي.
4. **القابلية للتحليل والتتبع:** البيانات الرقمية يمكن دمجها وتحليلها لإنتاج معلومات شخصية إضافية.

### المبحث الثاني: الطبيعة القانونية للحق في حماية البيانات

- **اتجاه الملكية:** بعض الفقه يرى البيانات حق ملكية معلوماتية.
- **اتجاه الحقوق اللصيقة بالشخصية:** الحق مشتق من الخصوصية، وهو الأكثر قبولاً، ويطبقه النظام السعودي والمصري والأوروبي.
- **التحليل:** حماية البيانات جزء من حماية حقوق الإنسان وكرامته، وليس مجرد سلعة تجارية.

## الباب الثاني: الحماية النظامية والقانونية للبيانات الشخصية

### الفصل الأول: التزامات جهة التحكم والمعالجة

#### المبحث الأول: مبادئ المعالجة المشروعة

1. مبدأ الغرض: جمع البيانات لأغراض محددة وواضحة.
2. مبدأ الحد الأدنى: الاكتفاء بالبيانات الضرورية فقط.
3. مبدأ الجودة والدقة: تحديث البيانات لمنع اتخاذ قرارات خاطئة.
4. توسعة: التزامات الرقابة الداخلية، مراجعة دورية للبيانات، وضمان شفافية التعامل عند نقل البيانات لدول أخرى.

#### المبحث الثاني: الالتزامات التقنية والإدارية

- السرية: منع وصول غير المخولين للبيانات.
- الإبلاغ عن التسريب: إشعار الجهات المختصة وصاحب البيانات فور حدوث الاختراق.
- توسعة: الالتزام بالتشفير، النسخ الاحتياطية، مراجعة سجلات الدخول، ومراقبة النشاطات المشبوهة.

## الفصل الثاني: حقوق صاحب البيانات وآليات ممارستها

### المبحث الأول: الحق في العلم والوصول

- معرفة من يجمع البيانات ولماذا.
- الحق في الوصول لنسخة البيانات بدون رسوم.

### المبحث الثاني: الحقوق التصحيحية والنهائية

1. الحق في التصحيح: تعديل البيانات أو استكمال الناقصة.
  2. الحق في الإزالة (النسيان): مسح البيانات عند انتهاء الغرض أو سحب الموافقة.
  3. توسعة: الحق في الاعتراض على المعالجة، نقل البيانات لجهة أخرى، وحالات عملية على المنصات الرقمية.
-

## الباب الثالث: المسؤولية القانونية عن انتهاك البيانات الشخصية

### الفصل الأول: أركان المسؤولية التقصيرية

#### المبحث الأول: الخطأ في معالجة البيانات

- تعريف الخطأ الرقمي: إخلال بالالتزامات القانونية.
- صور الخطأ: إيجابي (معالجة غير مصرح بها)، سلبي (إهمال الإجراءات التقنية).
- معيار الخطأ: المعيار المهني للشخص المتخصص أو الشركة التقنية الكبرى.

#### المبحث الثاني: الضرر وعلاقة السببية

- الضرر المادي: سرقة أرقام بطاقات، خسائر مالية.
- الضرر المعنوي: أذى نفسي وسمعة.
- إشكالية السببية: صعوبة إثبات المسؤولية عند تعدد الأطراف.

---

### الفصل الثاني: الجزاءات وآليات التعويض

#### المبحث الأول: المسؤولية الجنائية

- السعودية: غرامات تصل ٥ مليون ريال وسجن حتى سنتين، مصادرة أجهزة، تشهير.
- مصر: غرامات وحبس بحسب جسامة الجرم، مضاعفة العقوبة في حال العود.

#### المبحث الثاني: المسؤولية المدنية والتعويض

- دعوى التعويض: تقدير حجم الضرر وجسامة الخطأ والاستفادة من الانتهاك.
  - توسعة: إنشاء صناديق تعويض للضحايا مجهولي المصدر، ونماذج تقييم أضرار مالية ومعنوية موسعة.
-

## الخاتمة والتوصيات

### النتائج

1. البيانات امتداد للذات البشرية وحمايتها جزء من حماية حقوق الإنسان.
2. السعودية ومصر اعتمدتا معايير مشابهة GDPR مع مراعاة الخصوصية الوطنية.
3. الجزاءات المالية أكثر استخداماً للردع مقارنة بالسجن.

### التوصيات

1. تفعيل القضاء التقني المتخصص.
2. نشر التوعية حول سياسات الخصوصية.
3. إنشاء صناديق تعويض للانتهاكات مجهولة المصدر.
4. اقتراح تشريعات مستقبلية لتغطية ثغرات جديدة في البيئة الرقمية.

## قائمة المصادر والمراجع

1. نظام حماية البيانات الشخصية السعودي، المرسوم الملكي رقم (م/٤٧)، وتعديلاته.
2. اللائحة التنفيذية لنظام حماية البيانات الشخصية، الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا).
3. القانون المصري رقم ١٥١ لسنة ٢٠٢٠، بشأن حماية البيانات الشخصية.
4. اللائحة العامة لحماية البيانات (GDPR)، البرلمان الأوروبي والمجلس، ٢٠١٦.
5. د. خالد ممدوح، الحماية القانونية للبيانات الشخصية في المعاملات الإلكترونية، دار الفكر الجامعي، الإسكندرية.
6. د. محمد السعيد رشدي، المسؤولية المدنية عن أخطاء تكنولوجيا المعلومات، دار النهضة العربية، القاهرة.
7. د. عبد الفتاح بيومي حجازي، النظام القانوني لحماية الخصوصية في عصر الإنترنت، دار الفكر الجامعي.
8. د. طارق إبراهيم الدسوقي، أمن المعلومات والحماية القانونية للبيانات الشخصية، دار الجامعة الجديدة.

9. مجلة الدراسات القانونية، "المسؤولية التقصيرية في الفضاء السيبراني"، جامعة الملك سعود.

10. المجلة الدولية للقانون، "الحماية الجنائية للبيانات الحيوية في الأنظمة العربية."

### الملخص باللغة العربية:

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

### Abstract (English):

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