DOI: https://doi.org/10.33193/JALHSS.126.2025.1576
ISSN Online: 2414-3383
ISSN Print: 2616-3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
editor@jalhss.com
Volume (126) November 2025
العدد (126) نوفمبر 2025

حماية البيانات الشخصية في التطبيقات الإلكترونية والمنصات الرقمية في ضوء أحكام النظام السعودي والتشريعات المقارنة (نحو إطار قانوني أمثل لحماية بيانات المستهلك الإلكتروني)

د. حسام إبراهيم فلاتة
أستاذ القانون الخاص المشارك، جامعة جدة، المملكة العربية السعودية
البريد الالكتروني: Hifallatah@uj.edu.sa

الملخص

يتناول هذا البحث إشكالية حماية البيانات الشخصية للمستخدمين في التطبيقات الإلكترونية والمنصات الرقمية، من خلال دراسة مقارنة بين نظام حماية البيانات الشخصية السعودي واللائحة الأوروبية العامة لحماية البيانات (GDPR)، في ظل اعتماد نماذج الأعمال لهذه المنصات على الجمع المكثف للبيانات الشخصية وما يثيره ذلك من تحديات تتعلق بالخصوصية.

وتكمن أهمية البحث في تقييم مدى فعالية الإطار التشريعي السعودي الجديد في تنظيم الممارسات الفعلية لجمع ومعالجة البيانات من قبل هذه المنصات، وتحديدًا فيما يتعلق بآليات الحصول على الموافقة، واستخدام بيانات الموقع الجغرافي، وتحديد المسؤوليات القانونية للمنصة. ويسعى البحث إلى الإجابة عن إشكالية رئيسية: ما مدى كفاية الإطار القانوني الحالي في النظام السعودي لتوفير حماية فعالة لبيانات المستهلك الإلكتروني، وكيف يمكن تطوير آليات تطبيقه بالاستفادة من التجربة الأوروبية؟

ويعتمد البحث المنهج التحليلي المقارن، حيث يحلل نصوص نظام حماية البيانات الشخصية السعودي ولائحته التنفيذية، ويقارنها بالمبادئ الواردة في اللائحة الأوروبية. كما يتخذ البحث من منصات "أمازون"، "مرسول"، و"تويو" نماذج تطبيقية للدراسة، نظراً لطبيعة البيانات الحيوية التي تجمعها وحجم التحديات التي تفرضها على خصوصية المستخدم.

ويخلص البحث إلى عدة نتائج أهمها: أن نظام حماية البيانات الشخصية السعودي يضع إطاراً عاماً متيناً، إلا أن هناك فجوة في القواعد التنظيمية التفصيلية التي تعالج خصوصية نماذج عمل المنصات الرقمية، خاصة فيما يتعلق بوضوح آليات الموافقة وحدود استخدام البيانات الشخصية.

ويقدم البحث توصيات لتطوير المنظومة التشريعية تشمل: إصدار قواعد إرشادية لقطاعي التجارة الإلكترونية وخدمات التوصيل، تبني معايير واضحة للموافقة الصريحة والواعية، فرض التزامات تتعلق بالشفافية والخصوصية حسب التصميم، وتعزيز الدور الرقابي للهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA) لضمان الامتثال.

الكلمات المفتاحية : حماية البيانات الشخصية، المنصات الرقمية، الخصوصية، نظام حماية البيانات الشخصية السعودي، اللائحة الأوروبية العامة لحماية البيانات(GDPR) ، الموافقة، حماية المستهلك الإلكتروني، أمازون، مرسول.

DOI: https://doi.org/10.33193/JALHSS.126.2025.1576
ISSN Online: 2414-3383
ISSN Print: 2616-3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
editor@jalhss.com
Volume (126) November 2025
العدد (126) نوفمبر 2025

Personal Data Protection in Electronic Applications and Digital Platforms in Light of Saudi Law and Comparative Legislation

(Towards an Optimal Legal Framework for Protecting Electronic Consumer Data)

Dr. Hussam Ibrahim Hifallatah
Associate Professor of Private Law, Jeddah University, Kingdom of Saudi Arabia
Email: Hifallatah@uj.edu.sa

ABSTRACT

This research addresses the issue of protecting users' personal data in electronic applications and digital platforms through a comparative study between the Saudi Personal Data Protection Law and the European Union's General Data Protection Regulation (GDPR). This study is conducted in light of the reliance of these platforms' business models on the extensive collection of personal data and the resulting privacy challenges .The research's significance lies in evaluating the effectiveness of the new Saudi legislative framework in regulating the actual practices of data collection and processing by these platforms, specifically regarding consent mechanisms, the use of geolocation data, and defining the platform's legal responsibilities. The research seeks to answer a key question: To what extent is the current legal framework in the Saudi system sufficient to provide effective protection for electronic consumer data, and how can its implementation mechanisms be improved by drawing on the European experience? This research employs a comparative analytical approach, analyzing the texts of the Saudi Personal Data Protection Law and its implementing regulations, and comparing them with the principles outlined in the European regulations. The research also uses the Amazon, Mrsool, and Toyou platforms as case studies, given the nature of the biometric data they collect and the significant challenges they pose to user privacy .The research concludes with several key findings, most notably that while the Saudi Personal Data Protection Law provides a robust general framework, there is a gap in the detailed regulations addressing the privacy aspects of digital platform business models, particularly regarding the clarity of consent mechanisms and the limits of personal data use .

Keywords: Personal data protection, digital platforms, privacy, Saudi Personal Data Protection System, European General Data Protection Regulation (GDPR), consent, e-consumer protection, Amazon, Mrsool**.**

DOI: https://doi.org/10.33193/JALHSS.126.2025.1576
ISSN Online: 2414-3383
ISSN Print: 2616-3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
editor@jalhss.com
Volume (126) November 2025
العدد (126) نوفمبر 2025

المقدمة

شهدت السنوات الأخيرة قفزة هائلة في تبني التقنيات الرقمية على مستوى العالم، حيث أصبح الاقتصاد الرقمي محركاً أساسياً للنمو. وفي المملكة العربية السعودية، يتسارع هذا التحول بشكل ملحوظ استجابةً لمستهدفات رؤية المملكة 2030، حيث من المتوقع أن يساهم الاقتصاد الرقمي بحوالي 19.4% من الناتج المحلي الإجمالي بحلول عام 2025. وقد أدى هذا التحول إلى انتشار واسع للتطبيقات الإلكترونية والمنصات الرقمية التي أصبحت جزءاً لا يتجزأ من حياة المستهلكين اليومية[1].

وتلعب هذه المنصات، مثل "أمازون" للتجارة الإلكترونية و"مرسول" و"تويو" لخدمات التوصيل، دوراً محورياً في هذا الاقتصاد الجديد. فهي لا تقتصر على تقديم خدمة أو سلعة، بل إن نماذج أعمالها تعتمد بشكل أساسي على جمع ومعالجة كميات ضخمة من بيانات المستخدمين الشخصية، والتي تُعتبر بحق "النفط الجديد" في العصر الرقمي. غير أن هذا الدور المتنامي للمنصات يثير إشكاليات قانونية معقدة فيما يتعلق بحماية خصوصية المستخدمين وحدود استخدام بياناتهم، خاصة في ظل جمع بيانات حساسة مثل سجلات الشراء وتفضيلات البحث وبيانات الموقع الجغرافي الدقيقة[2].

تبرز أهمية هذا الموضوع من الناحية النظرية في كونه يتناول إشكالية قانونية معاصرة تتمثل في مدى قدرة الأطر التشريعية التقليدية والحديثة على تنظيم ممارسات تقنية معقدة قائمة على البيانات. أما من الناحية العملية، فإن غياب قواعد واضحة ومفصلة لكيفية تطبيق مبادئ حماية البيانات يترتب عليه مخاطر متعددة تهدد خصوصية المستهلكين، بدءاً من الاستهداف الإعلاني المفرط وصولاً إلى التنميط السلوكي وإمكانية إساءة استخدام البيانات.[3]

وفي حين رسخت اللائحة الأوروبية العامة لحماية البيانات (GDPR) معياراً عالمياً صارماً في هذا المجال، فإن النظام السعودي لحماية البيانات الشخصية، الصادر عام 2021 والذي دخل حيز التنفيذ في 2023، لا يزال حديث العهد، ولم تتبلور بعد تطبيقاته القضائية والتنظيمية بشكل كامل، خاصة فيما يتعلق بآليات الموافقة ونطاقها في بيئة التطبيقات الرقمية. هذا الوضع يستدعي دراسة تحليلية مقارنة لاستخلاص الدروس المستفادة وتقديم الإضافات المقترحة لضمان بناء إطار قانوني أمثل يوفر حماية فعالة لبيانات المستهلك الإلكتروني في المملكة.[4]

إشكالية البحث وتساؤلاته

تتمحور إشكالية البحث الرئيسية حول مدى كفاية الإطار القانوني السعودي، ممثلاً بنظام حماية البيانات الشخصية ولائحته التنفيذية، في تنظيم ممارسات جمع ومعالجة البيانات الشخصية من قبل التطبيقات الإلكترونية والمنصات الرقمية، وكيف يمكن تطوير هذا الإطار لتحقيق حماية مثلى للمستهلك الإلكتروني بالاستفادة من التجربة الأوروبية؟

وتتفرع عن هذه الإشكالية مجموعة من التساؤلات الفرعية:

1. ما هي طبيعة وأنواع البيانات الشخصية التي تجمعها المنصات الرقمية، وما هي الأسس القانونية التي تستند إليها في معالجتها لتحقيق نماذج أعمالها؟
2. ما هي أبرز المبادئ والالتزامات التي أرستها اللائحة الأوروبية العامة لحماية البيانات (GDPR) فيما يتعلق بموافقة المستخدم، والشفافية، والخصوصية حسب التصميم؟
3. إلى أي مدى يوفر نظام حماية البيانات الشخصية السعودي ولائحته التنفيذية حماية كافية للمستهلك، خاصة فيما يتعلق بآليات الحصول على الموافقة الصريحة، وحماية بيانات الموقع الجغرافي؟
4. ما هي أبرز الفجوات التشريعية أو التحديات التطبيقية في النظام السعودي عند مقارنته بالمعايير التي وضعتها اللائحة الأوروبية(GDPR) ؟

[1] منظمة التعاون الرقمي، تقرير حالة الاقتصاد الرقمي في المملكة العربية السعودية 2023: ازدهار رقمي للجميع. الرياض، المملكة العربية السعودية: منظمة التعاون الرقمي، 2023، ص. 4.

[2] Zuboff, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019, p. 8

[3] Solove, Daniel J. "The Myth of the Privacy Paradox." George Washington Law Review, Vol. 89, No. 1, 2021, p. 22.

[4] Kuner, Christopher, et al. "The GDPR as a model for global data protection law?" International Data Privacy Law, Vol. 12, Issue 1, February 2022, p. 1

DOI: https://doi.org/10.33193/JALHSS.126.2025.1576
ISSN Online: 2414-3383
ISSN Print: 2616-3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
editor@jalhss.com
Volume (126) November 2025
العدد (126) نوفمبر 2025

5. ما هي المعايير القانونية والتقنية التي يمكن الاستناد إليها لتحديد المسؤوليات على المنصات الرقمية باعتبارها "متحكم بيانات"؟
6. ما هي الالتزامات المحددة التي يُقترح فرضها على المنصات لضمان الشفافية، وتقليل جمع البيانات، وتوفير خيارات تحكم فعالة للمستخدمين؟
7. ما هي الآليات الرقابية والتنظيمية المقترحة لتطوير إنفاذ نظام حماية البيانات الشخصية السعودي وتعزيز دوره في حماية المستهلك الإلكتروني؟

منهجية البحث

يعتمد البحث على **المنهج التحليلي المقارن**، حيث يقوم بتحليل النصوص النظامية في كل من نظام حماية البيانات الشخصية السعودي ولائحته التنفيذية، واللائحة الأوروبية العامة لحماية البيانات(GDPR) ، ومقارنة موقف كل منهما من المبادئ الأساسية لمعالجة البيانات، وحقوق أصحابها، والتزامات المنصات الرقمية. كما يستخدم البحث **المنهج التحليلي التطبيقي**، من خلال فحص وتقييم سياسات الخصوصية وشروط الاستخدام التي تطبقها المنصات الرقمية محل الدراسة، بهدف تحديد آليات جمع البيانات والموافقة المتبعة عملياً، ومدى توافقها مع المتطلبات النظامية.

ويتبنى البحث أيضاً **منهج دراسة الحالة** من خلال التركيز على نماذج منصات "أمازون"، "مرسول"، و"تويو". ويأتي اختيار هذه المنصات لكونها تمثل قطاعات مختلفة (التجارة الإلكترونية وخدمات التوصيل) وتعتمد بشكل مكثف على أنواع متباينة من البيانات الشخصية (سجل المشتريات، بيانات الموقع الجغرافي)، مما يوفر مادة ثرية ومتنوعة للتحليل التطبيقي.

خطة البحث:

تنقسم خطة الدراسة إلى مبحثين على النحو التالي:

المبحث الأول: الإطار المفاهيمي والنظامي لحماية البيانات الشخصية في المنصات الرقمية

المبحث الثاني: تقييم فعالية النظام السعودي واقتراح آليات تطويرية في ضوء التشريعات المقارنة والتطبيقات العملية

المبحث الأول: الإطار المفاهيمي والقانوني لحماية البيانات الشخصية في المنصات الرقمية السعودية

يتناول هذا المبحث الأسس النظرية والنظامية التي تحكم حماية البيانات الشخصية في بيئة المنصات الرقمية، مسلطا الضوء على طبيعة هذه البيانات وكيفية تحولها إلى أصول اقتصادية، والمخاطر المترتبة على ذلك. كما يستعرض المبحث الإطار الذي وضعه المشرع السعودي من خلال نظام حماية البيانات الشخصية لتنظيم هذا القطاع الحيوي، وتحديد المبادئ الحاكمة والحقوق والالتزامات المترتبة على أطراف العلاقة.

1. ماهية البيانات الشخصية في الاقتصاد الرقمي ونماذج عمل المنصات:

1.1 تعريف البيانات الشخصية وتصنيفاتها (البيانات الحساسة، بيانات الموقع الجغرافي):

يعرف نظام حماية البيانات الشخصية السعودي البيانات الشخصية بأنها كل بيان مهما كان مصدره أو شكله، من شأنه أن يؤدي إلى معرفة الفرد على وجه التحديد، أو يجعله قابلا للتعرف عليه بصفة مباشرة أو غير مباشرة. ويشمل ذلك الاسم، ورقم الهوية، والعناوين، وأرقام التواصل، والصور الشخصية. ويميز النظام فئة خاصة من البيانات وهي البيانات الحساسة التي تشير إلى الأصل العرقي أو القبلي للفرد، أو معتقداته الدينية أو الفكرية، بالإضافة إلى البيانات الصحية والبيانات الائتمانية والبيانات الجنائية، وقد أولاها حماية مشددة. وتبرز في سياق المنصات الرقمية أهمية بيانات الموقع الجغرافي التي، ورغم عدم تصنيفها صراحة كبيانات حساسة في النظام، إلا أنها قد تكشف عن تفاصيل دقيقة تتعلق بحياة الفرد وسلوكياته، مما يجعلها ذات طبيعة حساسة تتطلب عناية خاصة.[5]

[5] المملكة العربية السعودية، نظام حماية البيانات الشخصية، الصادر بالمرسوم الملكي رقم (م/19) بتاريخ 1443/2/9هـ، المادة الأولى.

DOI: https://doi.org/10.33193/JALHSS.126.2025.1576
ISSN Online: 2414-3383
ISSN Print: 2616-3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
editor@jalhss.com
Volume (126) November 2025
العدد (126) نوفمبر 2025

1.2 نماذج الأعمال القائمة على البيانات: كيف تستخدم منصات (أمازون، مرسول، تويو) البيانات كأصل اقتصادي:

تعتمد نماذج الأعمال الحديثة للمنصات الرقمية بشكل جوهري على تحويل البيانات الشخصية للمستخدمين إلى أصول اقتصادية قابلة للاستثمار. تستخدم منصة أمازون بيانات سجلات الشراء والتصفح والبحث لتكوين ملفات تعريفية دقيقة عن المستهلكين، مما يمكنها من عرض إعلانات موجهة والتوصية بمنتجات محددة لزيادة المبيعات. وفي المقابل، تعتمد منصات مثل مرسول وتويو بشكل أساسي على بيانات الموقع الجغرافي اللحظية والتاريخية لتحسين كفاءة عمليات التوصيل، وفي الوقت نفسه تستغل هذه البيانات لفهم أنماط حركة وسلوك المستهلكين، وهو ما يمثل قيمة اقتصادية كبيرة يمكن استخدامها في تطوير خدمات جديدة أو مشاركتها مع أطراف ثالثة لأغراض تسويقية بعد الحصول على الموافقات اللازمة. [6]

1.3 المخاطر المترتبة على جمع البيانات: انتهاك الخصوصية، التنميط السلوكي، والأمن السيبراني:

يترتب على عمليات جمع ومعالجة البيانات الشخصية الواسعة التي تقوم بها المنصات الرقمية مجموعة من المخاطر الجوهرية التي تهدد حقوق الأفراد. يتمثل الخطر الأبرز في انتهاك الحق في الخصوصية من خلال تجميع كميات هائلة من البيانات التي قد تكشف أدق تفاصيل حياة الفرد. ويؤدي تحليل هذه البيانات إلى ممارسة التنميط السلوكي، حيث يتم تصنيف المستخدمين في فئات محددة بناء على سلوكياتهم وتفضيلاتهم، وقد يستخدم هذا التنميط للتأثير على قراراتهم الشرائية أو حتى استبعادهم من الحصول على خدمات معينة. بالإضافة إلى ذلك، يشكل تخزين هذا الكم الهائل من البيانات هدفا ثمينا للهجمات السيبرانية، حيث قد يؤدي أي اختراق أمني إلى تسريب بيانات ملايين المستخدمين واستخدامها في عمليات احتيال أو سرقة هوية. [7]

2. أسس الحماية في نظام حماية البيانات الشخصية السعودي:

2.1 نطاق تطبيق النظام على المنصات الرقمية:

يحدد نظام حماية البيانات الشخصية السعودي نطاق تطبيق واسع يضمن خضوع معظم المنصات الرقمية العاملة في المملكة لأحكامه. يسري النظام على أي عملية معالجة للبيانات الشخصية تتم داخل المملكة من قبل أي جهة، بما في ذلك المنصات المحلية مثل مرسول وتويو. والأهم من ذلك، يمتد نطاق تطبيق النظام خارج الحدود الإقليمية ليشمل أي جهة تقع خارج المملكة تقوم بمعالجة بيانات شخصية تتعلق بأفراد مقيمين فيها، وهو ما يخضع المنصات العالمية مثل أمازون وغيرها من الشركات الأجنبية التي تقدم خدماتها للمستخدمين في السعودية لأحكام النظام والتزاماته بشكل مباشر. [8]

2.2 المبادئ الحاكمة لمعالجة البيانات (المشروعية، الشفافية، تحديد الغرض، الاكتفاء بالحد الأدنى):

يرسي النظام مجموعة من المبادئ الأساسية التي يجب على المنصات الرقمية الالتزام بها عند معالجة البيانات الشخصية لضمان حماية حقوق أصحابها. يتطلب مبدأ المشروعية وجود مسوغ نظامي واضح لجمع البيانات، وتعد موافقة صاحب البيانات هي المسوغ الأساسي. ويفرض مبدأ الشفافية على المنصات إبلاغ المستخدمين بشكل واضح وصريح بطبيعة البيانات التي تجمعها والغرض منها. كما يلزم مبدأ تحديد الغرض بأن يكون جمع البيانات لغرض محدد ومعلن، وألا تتم معالجتها لاحقا بما يتنافى مع هذا الغرض. ويقضي مبدأ الاكتفاء بالحد الأدنى بأن تقتصر عملية جمع البيانات على الحد الأدنى اللازم لتحقيق الغرض المحدد، وتجنب جمع بيانات غير ضرورية. [9]

2.3 حقوق أصحاب البيانات (الحق في العلم، والوصول، والتصحيح، والإتلاف):

يمنح النظام أصحاب البيانات مجموعة من الحقوق الجوهرية التي تمكنهم من السيطرة على بياناتهم الشخصية. يشمل ذلك الحق في العلم، الذي يوجب على المنصات إخطار المستخدمين بالمسوغ النظامي لجمع بياناتهم

---

[6] Zuboff, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019, p. 94.

[7] Solove, Daniel J. Understanding Privacy. Cambridge, MA: Harvard University Press, 2008, p. 105

[8] المملكة العربية السعودية. اللائحة التنفيذية لنظام حماية البيانات الشخصية، الصادرة بقرار مجلس إدارة الهيئة السعودية للبيانات والذكاء الاصطناعي رقم (1445/3) بتاريخ 1445/2/7هـ، المادة الثانية.

[9] المملكة العربية السعودية، نظام حماية البيانات الشخصية، الصادر بالمرسوم الملكي رقم (م/19) بتاريخ 1443/2/9هـ، المادة الخامسة عشر.

DOI: https://doi.org/10.33193/JALHSS.126.2025.1576
ISSN Online: 2414-3383
ISSN Print: 2616-3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
editor@jalhss.com
Volume (126) November 2025
العدد (126) نوفمبر 2025

والغرض منه. ويكفل النظام الحق في الوصول إلى البيانات الشخصية المحفوظة لدى المنصة والحصول على نسخة منها. كما يتيح الحق في طلب تصحيح البيانات غير الدقيقة أو غير المكتملة أو تحديثها. ويضمن النظام كذلك الحق في طلب إتلاف البيانات الشخصية في حالات محددة، كأن تكون البيانات لم تعد ضرورية لتحقيق الغرض الذي جمعت من أجله، أو عند سحب المستخدم لموافقته على معالجتها.[10]

2.4 التزامات "متحكم البيانات" ودور الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA:)

يفرض النظام التزامات واضحة على المنصات الرقمية باعتبارها "متحكم بيانات"، وهو الطرف الذي يحدد الغرض من معالجة البيانات الشخصية وكيفيتها. تشمل هذه الالتزامات ضمان دقة البيانات وأمنها، واتخاذ التدابير التنظيمية والتقنية اللازمة لحمايتها من التسريب أو التلف أو الوصول غير المشروع. كما يلزم النظام متحكم البيانات في حالات معينة بإجراء تقييم للأثر المترتب على معالجة البيانات، وتعيين مسؤول لحماية البيانات الشخصية. وتتولى الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) دور الجهة المختصة بالإشراف على تطبيق أحكام النظام، وتلقي البلاغات والشكاوى، وإصدار اللوائح والسياسات اللازمة لضمان حماية فعالة للبيانات الشخصية في المملكة.[11]

المبحث الثاني: تقييم فعالية حماية البيانات في تطبيقات ومنصات محددة وسبل التطوير في ضوء التجربة الأوروبية

ينتقل هذا المبحث من الإطار النظري إلى التحليل التطبيقي والمقارن، حيث يقيم الممارسات الفعلية لجمع البيانات في منصات رقمية محددة ويقارنها بالمعايير المتقدمة التي أرستها التجربة الأوروبية. ويهدف المبحث في نهايته إلى استخلاص الدروس المستفادة وتقديم توصيات محددة لبناء إطار قانوني أمثل يعزز حماية بيانات المستهلك الإلكتروني في المملكة.

1. دراسة حالة تطبيقية لممارسات جمع البيانات في المنصات:

1.1 تحليل سياسات الخصوصية لمنصة "أمازون": (بيانات سجل الشراء والتصفح):

تكشف سياسة الخصوصية الخاصة بمنصة أمازون عن منظومة واسعة لجمع البيانات تتجاوز المعلومات الأساسية التي يقدمها المستخدم عند إنشاء الحساب. تقوم المنصة بتسجيل وتحليل كل تفاعل للمستخدم داخل تطبيقها، بما في ذلك المنتجات التي يتم عرضها، ومدة النظر في كل صفحة، والمصطلحات المستخدمة في البحث، والمنتجات المضافة إلى سلة التسوق أو قائمة الرغبات، وسجل المشتريات الكامل. وتستخدم أمازون هذه البيانات بشكل مكثف لتشغيل محرك التوصيات الخاص بها، وتخصيص الواجهة الرئيسية لكل مستخدم، وعرض إعلانات شديدة الاستهداف، مما يحول بيانات التصفح والشراء إلى أداة أساسية لزيادة المبيعات وتعظيم الأرباح.[12]

1.2 تحليل سياسات الخصوصية لمنصتي "مرسول" و"تويو": (التركيز على بيانات الموقع الجغرافي):

تعتمد منصتا مرسول وتويو بشكل أساسي على جمع بيانات الموقع الجغرافي لتقديم خدماتهما في مجال التوصيل. وتوضح سياسات الخصوصية لهذه المنصات أنها تجمع بيانات الموقع بشكل دقيق ومستمر أثناء استخدام التطبيق لتحديد مواقع استلام وتسليم الطلبات، وتوجيه مندوبي التوصيل، وتقدير الأوقات اللازمة لإتمام المهمة. ويتجاوز الأمر ذلك إلى جمع بيانات عن مسارات التنقل المعتادة للمستخدم وأنماط حركته، الأمر الذي يثير مخاوف جدية

[10] المملكة العربية السعودية، نظام حماية البيانات الشخصية، الصادر بالمرسوم الملكي رقم (م/19) بتاريخ 1443/2/9هـ، المادة الرابعة.

[11] المملكة العربية السعودية، اللائحة التنفيذية لنظام حماية البيانات الشخصية، الصادرة بقرار مجلس إدارة الهيئة السعودية للبيانات والذكاء الاصطناعي رقم (1445/3) بتاريخ 1445/2/7هـ، المادة السادسة والثلاثون.

[12] Crain, Matthew. Profit Over Privacy: How Amazon Uses Your Data to Make a Killing. University of Illinois Press, 2021, p. 55.

DOI: https://doi.org/10.33193/JALHSS.126.2025.1576
ISSN Online: 2414-3383
ISSN Print: 2616-3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
editor@jalhss.com
Volume (126) November 2025
العدد (126) نوفمبر 2025

تتعلق بالخصوصية، حيث يمكن أن ترسم هذه البيانات صورة متكاملة عن حياة الفرد وروتينه اليومي، مثل مكان سكنه وعمله والأماكن التي يتردد عليها باستمرار.[13]

1.3 تقييم آليات الحصول على "الموافقة" في المنصات الثلاث ومدى توافقها مع النظام:

تثير آليات الحصول على موافقة المستخدم في المنصات الثلاث إشكاليات جوهرية عند مقارنتها بمتطلبات الموافقة الصريحة والواعية التي نص عليها نظام حماية البيانات الشخصية السعودي. ففي الغالب، تتبع هذه المنصات نهج الموافقة الشاملة أو "المجمعة"، حيث يضطر المستخدم للموافقة على سياسة خصوصية طويلة ومعقدة كشرط أساسي لاستخدام الخدمة، دون منحه خيارا لقبول بعض ممارسات جمع البيانات ورفض البعض الآخر. ويؤدي هذا الأسلوب إلى إضعاف مفهوم الموافقة الحرة، حيث يشعر المستخدم بأنه مجبر على القبول للاستفادة من الخدمة، مما يجعل موافقته شكلية أكثر من كونها تعبيرا حقيقيا عن إرادة واعية ومستنيرة. [14]

2. دراسة مقارنة مع اللائحة الأوروبية العامة لحماية البيانات(GDPR):

2.1 مفهوم الموافقة الصريحة والمجزأة (Granular Consent)في اللائحة الأوروبية:

ترسخ اللائحة الأوروبية العامة لحماية البيانات معيارا متقدما للموافقة يتجاوز مجرد القبول العام. ويتطلب الحصول على موافقة صالحة بموجب اللائحة أن تكون حرة، ومحددة، ومستنيرة، ولا لبس فيها، وأن يتم التعبير عنها من خلال بيان واضح أو عمل إيجابي صريح. والأهم من ذلك، تؤكد اللائحة على ضرورة الموافقة المجزأة، والتي تعني وجوب منح المستخدم القدرة على الموافقة بشكل منفصل على كل غرض من أغراض معالجة البيانات. وبموجب هذا المفهوم، لا يجوز للمنصة أن تطلب موافقة واحدة وشاملة لمعالجة البيانات لأغراض تشغيلية وتسويقية وتحليلية معا، بل يجب أن توفر خيارات واضحة ومستقلة لكل غرض.[15]

2.2 مبادئ الخصوصية حسب التصميم والخصوصية الافتراضية (Privacy by Design & by Default):

يؤسس التشريع الأوروبي لمبدأين استباقيين لضمان حماية البيانات منذ المراحل الأولى. يتطلب مبدأ الخصوصية حسب التصميم من المنصات دمج تدابير حماية البيانات في صميم أنظمتها وخدماتها منذ بداية عملية التصميم، بدلا من محاولة إضافتها لاحقا. ويكمل هذا المبدأ مبدأ الخصوصية الافتراضية، الذي يقضي بضرورة أن تكون الإعدادات الأولية لأي منتج أو خدمة هي الأكثر حماية للخصوصية بشكل تلقائي، دون الحاجة إلى تدخل من المستخدم. ويعني ذلك، على سبيل المثال، أن خيارات مشاركة البيانات مع أطراف ثالثة أو استخدامها لأغراض تسويقية يجب أن تكون معطلة بشكل افتراضي، وعلى المستخدم تفعيلها بنفسه إذا رغب في ذلك.[16]

2.3 ضوابط التنميط الآلي (Automated Profiling)واتخاذ القرارات:

تضع اللائحة الأوروبية ضوابط مشددة على عمليات التنميط واتخاذ القرارات المؤتمتة بالكامل التي قد تترتب عليها آثار قانونية أو خطيرة على الأفراد. وتمنح اللائحة الأفراد الحق في عدم الخضوع لقرار يستند فقط إلى معالجة آلية، بما في ذلك التنميط، إذا كان هذا القرار ينتج آثارا قانونية ضدهم أو يؤثر عليهم بشكل كبير. وينطبق هذا المبدأ بشكل مباشر على المنصات التي قد تستخدم الخوارزميات لتقييم الجدارة الائتمانية للمستخدمين، أو تحديد أسعار الخدمات بشكل فردي، أو حتى رفض تقديم الخدمة لهم، حيث يجب أن توفر هذه المنصات الحق في التدخل البشري والتعبير عن وجهة النظر والاعتراض على القرار المؤتمت.[17]

---

[13] Richmond, Riva, and Bart van der Sloot. "The Legal Framework for Location Data in the Digital Age." In Privacy and Data Protection in an Age of Hyper-Connectivity, edited by David Lyon and Zygmunt Bauman, Edward Elgar Publishing, 2020, p. 112.

[14] Acquisti, Alessandro, Curtis Taylor, and Liad Wagman. "The Economics of Privacy." Journal of Economic Literature, Vol. 54, No. 2, June 2016, p. 450.

[15] Voigt, Paul, and Axel von dem Bussche. The EU General Data Protection Regulation (GDPR): A Practical Guide. Springer International Publishing, 2017, p. 99.

[16] Schartum, Dag Wiese. "Making Privacy by Design Operative." International Journal of Law and Information Technology, Vol. 24, Issue 2, Summer 2016, p. 155.

[17] Kaminski, Margot E., and Gianclaudio Malgieri. "Algorithmic Impact Assessments under the GDPR: Producing Multi-layered Explanations." International Data Privacy Law, Vol. 11, Issue 2, May 2021, p. 128.

DOI: https://doi.org/10.33193/JALHSS.126.2025.1576
ISSN Online: 2414-3383
ISSN Print: 2616-3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
editor@jalhss.com
Volume (126) November 2025
العدد (126) نوفمبر 2025

2.4 تحديد أوجه القوة في التجربة الأوروبية التي يمكن الاستفادة منها سعوديًا:

تتجلى أوجه القوة في التجربة الأوروبية في عدة جوانب يمكن أن يستلهم منها المشرع السعودي لتطوير البيئة التشريعية. تتمثل القوة الأولى في تبني نهج قائم على المخاطر يفرض التزامات أشد على الجهات التي تقوم بأنشطة معالجة عالية الخطورة. وتكمن القوة الثانية في وضوح وتفصيل المتطلبات المتعلقة بالموافقة والشفافية، مما لا يترك مجالا كبيرا للتأويل. وتبرز القوة الثالثة في مبدأ المساءلة، الذي لا يكتفي بإلزام المنصات بالامتثال، بل يطالبها بالقدرة على إثبات هذا الامتثال في أي وقت. وأخيرا، يمثل وجود سلطات إشرافية وطنية مستقلة وذات صلاحيات واسعة في التحقيق وفرض العقوبات الرادعة حجر الزاوية في ضمان الإنفاذ الفعال لأحكام اللائحة.[18]

3. نحو إطار قانوني أمثل: توصيات لتطوير البيئة التشريعية:

3.1 توصيات تشريعية: تعديلات مقترحة على اللائحة التنفيذية

يقترح البحث النظر في إدخال تعديلات على اللائحة التنفيذية لنظام حماية البيانات الشخصية لزيادة مستوى الوضوح والحماية. يمكن أن تشمل هذه التعديلات النص صراحة على تبني مفهوم الموافقة المجزأة، ووضع تعريف أكثر تفصيلا لمتطلبات الموافقة الصريحة في البيئة الرقمية. كما يقترح إضافة أحكام تلزم المنصات بتبني مبادئ الخصوصية حسب التصميم والخصوصية الافتراضية، ووضع ضوابط محددة لمعالجة بيانات الموقع الجغرافي نظرا لطبيعتها الحساسة.[19]

3.2 توصيات تنظيمية: ضرورة إصدار قواعد إرشادية لقطاعي التجارة الإلكترونية والتوصيل:

يوصي البحث بأن تقوم الهيئة السعودية للبيانات والذكاء الاصطناعي بإصدار قواعد تنظيمية وإرشادية قطاعية موجهة لمنصات التجارة الإلكترونية وخدمات التوصيل. ويمكن لهذه القواعد أن تترجم المبادئ العامة الواردة في النظام ولائحته التنفيذية إلى ممارسات عملية وواضحة، كأن تحدد أفضل السبل لتصميم واجهات الحصول على الموافقة، وتضع أمثلة على الحد الأدنى من البيانات اللازمة لتقديم كل خدمة، وتوضح الالتزامات المتعلقة بالشفافية في استخدام الخوارزميات لأغراض التوصية والتسعير.[20]

3.3 توصيات للمنصات: أفضل الممارسات لتحقيق الامتثال وتعزيز ثقة المستخدم:

ينبغي على المنصات أن تتبنى نهجا استباقيا يتجاوز مجرد الامتثال للحد الأدنى من المتطلبات النظامية، وذلك من خلال تبني أفضل الممارسات العالمية في حماية الخصوصية. يشمل ذلك تصميم سياسات خصوصية موجزة وواضحة وسهلة الفهم، وتوفير لوحات تحكم تتيح للمستخدمين إدارة أذونات البيانات الخاصة بهم بسهولة ويسر، وتقديم شروحات مبسطة حول كيفية استخدام بياناتهم، والاستثمار في تقنيات تعزيز الخصوصية التي تقلل من كمية البيانات الشخصية المجمعة. إن بناء علاقة قائمة على الشفافية والثقة مع المستخدمين لم يعد خيارا، بل أصبح ميزة تنافسية أساسية.[21]

3.4 توصيات للمستهلكين: تعزيز الوعي بالحقوق الرقمية:

يقتضي تحقيق حماية فعالة للبيانات تضافر الجهود من جانب المستهلكين أنفسهم، وذلك من خلال رفع مستوى وعيهم بحقوقهم الرقمية. ويتوجب على الجهات المعنية، بما في ذلك الجهات الحكومية وجمعيات حماية المستهلك، إطلاق حملات توعوية مكثفة لتعريف المستهلكين بحقوقهم التي يكفلها لهم النظام، مثل الحق في الوصول إلى بياناتهم وتصحيحها وحذفها، وكيفية ممارسة هذه الحقوق، والإجراءات المتاحة لتقديم الشكاوى في

[18] De Hert, Paul, and Vagelis Papakonstantinou. "The new General Data Protection Regulation: Still a sound system for the protection of individuals?" Computer Law & Security Review, Vol. 32, Issue 2, April 2016, p. 185.

[19] Edwards, Lilian. "Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective." Common Market Law Review, Vol. 53, Issue 1, February 2016, p. 80.

[20] Hildebrandt, Mireille. "The new imbroglio: the citizen and the state in the era of data-driven agency." In Data Protection and Privacy: The Age of Intelligent Machines, edited by Ronald Leenes et al., Hart Publishing, 2018, p. 45.

[21] Martin, Kirsten E. "Ethical issues in the big data industry." MIS Quarterly Executive, Vol. 14, Issue 2, June 2015, p. 70.

DOI: https://doi.org/10.33193/JALHSS.126.2025.1576
ISSN Online: 2414-3383
ISSN Print: 2616-3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
editor@jalhss.com
Volume (126) November 2025
العدد (126) نوفمبر 2025

حال تعرض خصوصيتهم للانتهاك. إن تمكين المستهلكين بالمعرفة هو خط الدفاع الأول لضمان بيئة رقمية آمنة وعادلة للجميع.[22]

الخاتمة

تخلص هذه الدراسة إلى الأهمية القصوى لوجود إطار قانوني وتنظيمي مفصل وفعال لحماية البيانات الشخصية في المملكة العربية السعودية، خاصة في ظل هيمنة التطبيقات الإلكترونية والمنصات الرقمية التي تعتمد نماذج أعمالها على استغلال هذه البيانات. ومن خلال الدراسة المقارنة بين نظام حماية البيانات الشخصية السعودي واللائحة الأوروبية العامة لحماية البيانات(GDPR) ، وباستخدام منصات "أمازون" و"مرسول" و"تويو" كنماذج تطبيقية، كشف البحث عن أن التجربة الأوروبية تقدم إطاراً ناضجاً يرتكز على مبادئ استباقية وآليات متقدمة تضمن أن تكون موافقة المستخدم حقيقية ومستنيرة.

وفي المقابل، أبرز البحث أنه على الرغم من أن النظام السعودي يضع أساساً تشريعياً قوياً ومبادئ عامة متوافقة مع أفضل المعايير الدولية، إلا أن هناك فجوة في القواعد التطبيقية التفصيلية التي تعالج الممارسات المعقدة لهذه المنصات. إن الاعتماد على آليات الموافقة الشاملة والمبهمة، والجمع المكثف لبيانات حساسة كالموقع الجغرافي دون ضوابط قطاعية واضحة، يخلق حالة من الغموض قد تضعف من فعالية الحماية التي يهدف النظام إلى تحقيقها، وتهدد ثقة المستخدم في الاقتصاد الرقمي.

ويقترح البحث تبني مقاربة تطويرية متكاملة في النظام السعودي، تأخذ في الاعتبار الدروس المستفادة من التجارب الدولية كالتجربة الأوروبية، مع تكييفها لتناسب السياق المحلي المتسارع النمو. ترتكز هذه المقاربة على تعزيز الشفافية، وتفعيل مفهوم الموافقة الحقيقية، وفرض التزامات واضحة على المنصات بتبني الخصوصية كإعداد افتراضي، وتطوير آليات رقابية متخصصة، بما يضمن تحقيق توازن دقيق بين تشجيع الابتكار وحماية الحق الأصيل للأفراد في خصوصية بياناتهم، ويسهم في تحقيق مستهدفات رؤية المملكة 2030 نحو بناء اقتصاد رقمي آمن وموثوق.

وقد توصلت الدراسة إلى العديد من النتائج، كما أوصت الدراسة بالعديد من التوصيات، وذلك على النحو التالي:

أولاً: النتائج:

من أهم النتائج التي توصلت إليها الدراسة مايلي:

1. يعتمد نمو الاقتصاد الرقمي في المملكة بشكل مباشر على البيانات، مما يجعل وجود إطار تنظيمي مفصل لحماية هذه البيانات ضرورة استراتيجية وليس مجرد ضرورة قانونية.
2. يضع نظام حماية البيانات الشخصية السعودي مبادئ عامة قوية، لكنه يفتقر إلى قواعد تفصيلية كافية لتنظيم الممارسات الخاصة بالمنصات الرقمية، مثل التنميط السلوكي ومعالجة بيانات الموقع الجغرافي لأغراض غير تشغيلية.
3. آليات "الموافقة" المتبعة حالياً من قبل العديد من المنصات لا ترقى إلى مستوى الموافقة الحرة والمستنيرة والمحددة التي يتطلبها النظام، وغالباً ما تكون شرطاً شاملاً ومجبراً لاستخدام الخدمة.
4. تفتقر البيئة التشريعية السعودية إلى إلزام واضح بتبني مبادئ "الخصوصية حسب التصميم" و"الخصوصية الافتراضية"، مما يضع عبء حماية البيانات على المستخدم بدلاً من المنصة.
5. تقدم اللائحة الأوروبية العامة لحماية البيانات (GDPR) مفاهيم متقدمة يمكن الاستفادة منها مباشرة، مثل "الموافقة المجزأة"، وضوابط اتخاذ القرارات المؤتمتة، ومبدأ المساءلة الذي يتطلب من المنصات إثبات امتثالها.
6. تجمع منصات مثل أمازون ومرسول وتويو كميات هائلة من البيانات (سجل التصفح، الموقع الدقيق) تتجاوز ما هو ضروري بشكل صارم لتقديم الخدمة الأساسية، مما يخلق مخاطر خصوصية كبيرة.
7. يتطلب ضمان حقوق أصحاب البيانات (مثل الحق في الوصول والإتلاف) وجود آليات تقنية واضحة وسهلة الاستخدام من قبل المنصات، وهو ما لا يتوفر دائماً بالشكل المطلوب.

[22] Turow, Joseph. The Aisles Have Eyes: How Retailers Track Your Shopping, Strip Your Privacy, and Define Your Power. Yale University Press, 2017, p. 225.

DOI: https://doi.org/10.33193/JALHSS.126.2025.1576
ISSN Online: 2414-3383
ISSN Print: 2616-3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
editor@jalhss.com
Volume (126) November 2025
العدد (126) نوفمبر 2025

8. يتطلب تحقيق حماية فعالة بناء قدرات تنظيمية ورقابية متخصصة لدى الهيئة السعودية للبيانات والذكاء الاصطناعي (SDAIA) قادرة على فهم نماذج الأعمال التقنية المعقدة والتدقيق فيها.

ثانياً: التوصيات:

من أهم التوصيات التي توصي بها الدراسة مايلي:

1. توصي الدراسة بتعديل اللائحة التنفيذية لنظام حماية البيانات الشخصية لتضمين نصوص صريحة تتبنى مفهوم "الموافقة المجزأة"، وتضع معايير واضحة للموافقة الصالحة في البيئة الرقمية.
2. النص على إلزام المنصات بتطبيق مبادئ "الخصوصية حسب التصميم" و"الخصوصية الافتراضية"، بحيث تكون الإعدادات الأكثر حماية للخصوصية هي الإعدادات التلقائية عند تقديم أي خدمة.
3. إصدار قواعد تنظيمية قطاعية من قبل الهيئة السعودية للبيانات والذكاء الاصطناعي(SDAIA) ، خاصة لقطاعي التجارة الإلكترونية وخدمات التوصيل، لوضع ضوابط صارمة على جمع واستخدام بيانات الموقع الجغرافي والتنميط السلوكي.
4. إلزام المنصات بتوفير "لوحات تحكم خصوصية" سهلة الاستخدام، تمكن المستخدمين من ممارسة حقوقهم في الوصول إلى بياناتهم وتصحيحها وحذفها وسحب الموافقة عليها بسهولة ويسر.
5. وضع قواعد إجرائية واضحة تتعلق بالشفافية في استخدام الخوارزميات، وإلزام المنصات بتقديم تفسيرات مبسطة للمستخدمين حول كيفية استخدام بياناتهم في عمليات التوصية والتسعير الشخصي.
6. تعزيز القدرات التقنية والفنية للجهات الرقابية (SDAIA) للقيام بعمليات تدقيق استباقية على المنصات الرقمية، والتأكد من امتثال أنظمتها وخوارزمياتها لمتطلبات النظام.
7. تشجيع استخدام آليات تسوية المنازعات البديلة عبر الإنترنت (ODR) لمعالجة شكاوى انتهاك الخصوصية بكفاءة وسرعة، مع تدريب متخصص للقضاة للنظر في القضايا المتعلقة بالبيانات.
8. إطلاق حملات توعية وطنية لتعريف المستهلكين بحقوقهم بموجب نظام حماية البيانات الشخصية، وتشجيع ثقافة المطالبة بالخصوصية كحق أساسي في العصر الرقمي.

المراجع

1. اللائحة التنفيذية لنظام حماية البيانات الشخصية، الصادرة بقرار مجلس إدارة الهيئة السعودية للبيانات والذكاء الاصطناعي رقم (1445/3) بتاريخ 1445/2/7هـ.
2. المملكة العربية السعودية .رؤية المملكة العربية السعودية 2030، متاحة على: https://www.vision2030.gov.sa.
3. منظمة التعاون الرقمي .تقرير حالة الاقتصاد الرقمي في المملكة العربية السعودية 2023: ازدهار رقمي للجميع .الرياض: منظمة التعاون الرقمي، 2023.
4. نظام حماية البيانات الشخصية السعودي، الصادر بالمرسوم الملكي رقم (م/19) بتاريخ 1443/2/9هـ، والمعدل بالمرسوم الملكي رقم (م/147) بتاريخ 1444/9/5هـ.
5. الهيئة السعودية للبيانات والذكاء الاصطناعي .(SDAIA) الدليل الإرشادي لحقوق أصحاب البيانات الشخصية .الرياض: سدايا، 2023.
6. Acquisti, Alessandro, Curtis Taylor, and Liad Wagman. "The Economics of Privacy." Journal of Economic Literature 54, no. 2 (2016): 442–492.
7. Crain, Matthew. Profit Over Privacy: How Amazon Uses Your Data to Make a Killing. Champaign: University of Illinois Press, 2021.
8. De Hert, Paul, and Vagelis Papakonstantinou. "The new General Data Protection Regulation: Still a sound system for the protection of individuals?" Computer Law & Security Review 32, no. 2 (2016): 179–194.
9. Edwards, Lilian. "Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective." Common Market Law Review 53, no. 1 (2016): 65–94.

DOI: https://doi.org/10.33193/JALHSS.126.2025.1576
ISSN Online: 2414-3383
ISSN Print: 2616-3810
مجلة الفنون والأدب وعلوم الإنسانيات والاجتماع
Journal of Arts, Literature, Humanities and Social Sciences
www.jalhss.com
editor@jalhss.com
Volume (126) November 2025
العدد (126) نوفمبر 2025

10. Hildebrandt, Mireille. "The new imbroglio: the citizen and the state in the era of data-driven agency." In Data Protection and Privacy: The Age of Intelligent Machines, edited by Ronald Leenes et al., 35–54. Oxford: Hart Publishing, 2018.
11. Kaminski, Margot E., and Gianclaudio Malgieri. "Algorithmic Impact Assessments under the GDPR: Producing Multi-layered Explanations." International Data Privacy Law 11, no. 2 (2021): 125–144.
12. Kuner, Christopher, et al. "The GDPR as a model for global data protection law?" International Data Privacy Law 12, no. 1 (2022): 1–3.
13. Martin, Kirsten E. "Ethical issues in the big data industry." MIS Quarterly Executive 14, no. 2 (2015): 67–80.
14. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation).
15. Richmond, Riva, and Bart van der Sloot. "The Legal Framework for Location Data in the Digital Age." In Privacy and Data Protection in an Age of Hyper-Connectivity, edited by David Lyon and Zygmunt Bauman, 105–128. Cheltenham: Edward Elgar Publishing, 2020.
16. Schartum, Dag Wiese. "Making Privacy by Design Operative." International Journal of Law and Information Technology 24, no. 2 (2016): 151–173.
17. Solove, Daniel J. Understanding Privacy. Cambridge, MA: Harvard University Press, 2008.
18. Solove, Daniel J. "The Myth of the Privacy Paradox." George Washington Law Review 89, no. 1 (2021): 1–55.
19. Turow, Joseph. The Aisles Have Eyes: How Retailers Track Your Shopping, Strip Your Privacy, and Define Your Power. New Haven: Yale University Press, 2017.
20. Voigt, Paul, and Axel von dem Bussche. The EU General Data Protection Regulation (GDPR): A Practical Guide. Cham: Springer International Publishing, 2017.
21. Zuboff, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019.