الحماية التشريعية لخصوصية البيانات الرقمية في ظل قانون حماية خصوصية البيانات ١٥١ لسنة ٢٠٢٠م

Legislative Protection of Digital Privacy under the Data Privacy Law No. 151 of 2020

إعداد

د/ أحمد السيد الشوبري

أستاذ القانون المدني المساعد، كلية العلوم الإدارية والإنسانية، كليات بريدة، القصيم، المملكة العربية السعودية

الحماية التشريعية لخصوصية البيانات الرقمية
في ظل قانون حماية خصوصية البيانات ١٥١ لسنة ٢٠٢٠م

أحمد السيد الشوبري

قسم القانون المدني ، كلية العلوم الإدارية والإنسانية، كليات بريدة، القصيم، المملكة العربية السعودية.

البريد الإلكتروني :**Ahmed.Elshobry@bpc.edu.sa**

الملخص:

لقد أصبحت مسألة الحماية القانونية للخصوصية الرقمية ذات أهمية متزايدة في العصر الرقمي الحالي. مع الاستخدام الواسع النطاق للتكنولوجيا والإنترنت، حيث يقوم الأفراد بمشاركة المعلومات والبيانات الشخصية باستمرار عبر الإنترنت. ومع ذلك، يثير هذا الأمر مخاوف جادة بشأن خصوصية وأمن هذه المعلومات والبيانات. ونتيجة لذلك، دعت الحاجة المتزايدة إلى تشريعات شاملة تحمي حقوق خصوصية البيانات الرقمية للأفراد.

ولعل الاستخدام المتزايد لمنصات وسائل التواصل الاجتماعي، والمعاملات عبر الإنترنت، والأنشطة المعتمدة على الإنترنت، تعدى الامر مشاركة ملايين الأفراد المعلومات الشخصية بل يتركون بصمات رقمية لهم هذه التقنيات وأساليب الراحة الإلكترونية لها وجهين فهي تأتي بتكلفة كبيرة وهو خطر انتهاكات الخصوصية والوصول غير المصرح به إلى البيانات ومن أجل معالجة هذه المخاوف، نفذت الحكومات والمنظمات قوانين ولوائح مختلفة لحماية خصوصية البيانات الرقمية للأفراد، سعياً نحو إيجاد نوع من الحماية التشريعية والنظامية للبيانات.

يهدف هذا البحث إلى استكشاف مدى أهمية وكفاية الحماية القانونية للخصوصية الرقمية، وتحليل التشريعات القائمة لحماية البيانات الشخصية، بالإضافة إلى دراسة التحديات والفرص المتعلقة بهذا الموضوع في العصر الرقمي الحالي. ونسعى لتقديم توصيات لتعزيز الحماية القانونية للخصوصية الرقمية وتحقيق توازن بين الاستخدام الأمثل للتكنولوجيا والحفاظ على حقوق الأفراد.

<u>الكلمات المفتاحية</u>: الحماية القانونية ، خصوصية البيانات الرقمية ،أمن البيانات ، البيانات الشخصية، البيانات الحساسة ، التكنولوجيا الرقمية ، حق النسيان الرقمي.

Legislative Protection of Digital Privacy under the Data Privacy Law No. 151 of 2020.

Ahmed Al-Sayed Al-Shoubri
Assistant Professor of Civil Law, College of Administrative Sciences and Humanities, Buraidah Colleges, Qassim, Kingdom of Saudi Arabia.
Email : Ahmed.Elshobry@bpc.edu.sa

Abstract:
The issue of legal protection for digital privacy has become increasingly significant in the current digital era. With the widespread use of technology and the internet, individuals are continuously sharing personal information and data online. However, this raises serious concerns about the privacy and security of this information and data. Consequently, there is an increasing need for comprehensive legislation to protect individuals' digital privacy rights.

With the emergence of social media platforms, online transactions, and internet-based activities, millions of individuals constantly share personal information and leave digital footprints. These technologies and conveniences come with a significant cost - the risk of privacy violations and unauthorized access to data. To address these concerns, governments and organizations have implemented various laws and regulations to protect individuals' digital privacy, aiming to establish a form of legislative and regulatory protection for data.

This research aims to explore the importance of legal protection for digital privacy, analyze existing legislation for personal data protection, and study the challenges and opportunities related to this topic in the current digital age. Through this research, we seek to provide effective recommendations to enhance the legal protection of digital privacy and achieve a balance between optimal technology use and safeguarding individuals' rights.

Keywords: Legal Protection , Digital Data Privacy , Data Security , Personal Data, Sensitive Data ,Digital Technology , Digital Right To Be Forgotten.

مقدمة:

تشكل خصوصية المعلومات عبر الشبكات الإلكترونية قضية حيوية في العصر الحالي بسبب الاعتماد المتزايد على التكنولوجيا والإنترنت في تبادل المعلومات والتواصل. وتتعلق مسألة خصوصية المعلومات بحماية البيانات الشخصية والحفاظ على سرية المعلومات أثناء نقلها وتخزينها ومعالجتها عبر الشبكات الإلكترونية. وهو ما يستلزم وجود ضمانات ضرورية لحماية خصوصية تداول المعلومات والبيانات عبر الشبكات الإلكترونية مثل تشفير البيانات الذي يعد أحد أهم الوسائل لضمان خصوصية المعلومات والبيانات أثناء نقلها عبر الشبكات باستخدام تقنيات التشفير، إلى جانب توفير بروتوكولات الأمان التي تستخدمها الشبكات الإلكترونية مثل **HTTPS** [1] لتأمين الاتصالات بين المستخدم والخادم وتطبيق إجراءات أمنية لمنع الاختراقات والهجمات السيبرانية على الشبكات وتحديث البرمجيات بانتظام واستخدام جدران الحماية وأنظمة الكشف عن التسلل.

كما وقد عنيت المواقع الإلكترونية أيضا بإدارة الهويات والوصول حيث ينبغي تقديم الوصول إلى المعلومات الحساسة بناءً على مبدأ الحاجة إليها، وتحديد الأذونات بدقة للتحكم فيمن يمكنه الوصول إلى المعلومات. والسعي الدائم لتوعية وتدريب المستخدمين بأهمية حماية خصوصيتهم

(١) تعني"**Hypertext Transfer Protocol Secure**"، وهو بروتوكول مستخدم لتبادل المعلومات عبر الويب وهو وسيلة شائعة ومهمة لتأمين الاتصالات بين المستخدم والخادم عبر الشبكة.

وتوفير تدريب لهم حول كيفية التعامل بأمان مع المعلومات الشخصية عبر الإنترنت.

إلى جانب هذه الإجراءات التقنية المذكورة لابد من إبراز دور سياسات الخصوصية والامتثال للقوانين حيث يجب أن تكون هناك سياسات واضحة للخصوصية تحدد كيفية جمع واستخدام المعلومات ومشاركتها ويجب أن تلتزم هذه السياسات بمتطلبات القوانين المحلية والدولية المتعلقة بحماية البيانات الشخصية من أي هجمات تستهدف الحصول على معلومات شخصية للمستخدمين

بشكل عام، تتطلب خصوصية المعلومات عبر الشبكات الإلكترونية توازنًا بين تبادل المعلومات بكفاءة والحفاظ على سرية وأمان تلك المعلومات وحمايتها تشريعياً، وهذا يستدعي جهودًا مستمرة من الأفراد والمنظمات والجهات التشريعية والتنظيمية.

أسباب البحث:

- نسعى من خلال هذا البحث إلى تحقيق الضمان القانوني للحفاظ على خصوصية المعلومات الشخصية والبيانات أثناء استخدامها ومعالجتها في البيئة الرقمية من خلال حماية حقوق الأفراد في الحفاظ على خصوصيتهم والسيطرة على بياناتهم الشخصية. والتحكم في كيفية جمع واستخدام بياناتهم من قبل المؤسسات والشركات.
- الإسهام والتوجيه في صياغة التشريعات واللوائح المتعلقة بحماية البيانات الشخصية. مما يساعد في تطوير نصوص قوانين توفر إطاراً قانونياً للشركات والمؤسسات للامتثال لمتطلبات الخصوصية والتصدي للتهديدات السيبرانية.

- سن تشريعات جديدة أو تعديل التشريع القائم للتعامل مع التحديات الناشئة في مجال حماية البيانات ويحفز على استخدام التكنولوجيا بثقة.
- تحقيق توازن بين استفادة المجتمع من التقنيات والبيانات وبين حماية حقوق الأفراد وخصوصياتهم، مما يسهم في تطوير بيئة رقمية آمنة ومستدامة في ظل حماية تشريعية فعالة.

أهداف البحث:

١. تحديد المفهوم القانوني للبيانات الشخصية وبيان مصدرها.
٢. بيان المخاطر الناشئ عن استخدام البيانات والتزامات المسؤولين عن معالجتها.
٣. استعراض واقع حماية البيانات الشخصية الالكترونية ومدى كفايتها في ظل التطور التكنولوجي والعولمة.
٤. القاء الضوء على حق النسيان الرقمي ودرجة الاعتراف القضائي به.

مشكلة البحث: تكمن مشكلة البحث في ضرورة التطوير المستمر لتوفير الحماية القانونية لخصوصية معلومات الرقمية لمستخدمي شبكات الانترنت؟ وإيجاد حلول المشكلات القانونية الناتجة عن استخدام مواقع الشبكات الاجتماعية، في ظل القانون المصري لحماية خصوصية البيانات ١٥١ لسنة ٢٠٢٠ م.

تتمثل إشكالية البحث في دراسة مدى كفاية حماية المشرع لهذا الحق وتحقيق غرض المشرع في حماية البيانات الشخصية الالكترونية وتحديد نطاق ومفهوم سرية البيانات الشخصية لما يعاصره هذا المجال من حداثة وتطور مستمرين.

تساؤلات البحث: من المفترض أن يجيب البحث عن عدد من التساؤلات وهي:

١. هل حماية خصوصية البيانات الرقمية لاقت معالجة قانونية كافية؟
٢. ما هي الخصوصية والبيانات الشخصية أو المعلومات الرقمية في التعاملات الالكترونية؟
٣. هل عالج القانون المعني الحماية المطلوبة للخصوصية الرقمية في مصر؟
٤. ما هي طبيعة المسؤولية عن تلف المعلومات الناتج عن التعدي على الخصوصية؟ أو عن ضياع المعلومات بسبب نشر صور المستخدم على مواقع التواصل الاجتماعي؟

أهمية البحث: تجدر أهمية البحث في توفير حماية متطورة تشريعياً للخصوصية الرقمية بعد تطور تقنية المعلومات وأثرها على الأمن الشخصي للحياة الخاصة بتوفير الحماية الكافية لهذا الحق تشريعياً.

المنهج البحثي: استند الباحث للمنهج التحليلي في استعراض النصوص القانونية المتعلقة بموضوع البحث من أجل اقتراح حلول للمشكلات التي يطرحها البحث والمنهج الوصفي في استعراض التحديات التقنية الحديثة وخطورتها على البيانات الشخصية واستعراض الآليات القانونية لحماية الحق في الخصوصية واستند إلى المنهج المقارن احياناً لمعرفة مكانة التشريع المقارن في موضوع البحث، كما تضمن البحث مناقشة الآراء الفقهية والحلول القضائية. وذلك من خلال مقدمة ومبحثين وخاتمة وتناول مجموعة من النتائج والتوصيات.

نطاق البحث: يشمل نطاق البحث حق خصوصية البيانات الشخصية وهو أحد الحقوق اللصيقة بالإنسان.

خطة البحث: تم تقسيم البحث الى مبحثين أساسيين تناولنا فيه:

المبحث الأول: مدلول خصوصية البيانات الرقمية والبيانات الشخصية والمخاطر التي تواجهها.

- ❖ **المطلب الأول:** المقصود بالبيانات الشخصية والاهتمامات التشريعية بها .
- ❖ **المطلب الثاني:** خصوصية البيانات الرقمية ومخاطرها

المبحث الثاني: انتهاك خصوصية البيانات الرقمية والمعالجة التشريعية

- **المطلب الأول:** التنظيم القانونية لحماية خصوصية البيانات الرقمية
- **المطلب الثاني:** حماية خصوصية البيانات الرقمية في القانون المصري

المبحث الأول

مدلول خصوصية البيانات الرقمية والبيانات الشخصية والمخاطر التي تواجهها

من الحقوق المعترف بها عالمياً الحق في حماية الحياة الخاصة وأمنها إلا أن التطور التكنولوجي أبان إمكانية الاعتداء على مثل هذه الحقوق ما لم يتم حمايتها قانوناً وتنظيم استخدامها وبيان سبل تداولها وتخزينها أو معالجة البيانات الشخصية للمتعاملين مع هذه التكنولوجيا بل ووضع أطر تحديد المسؤولية المدنية والجنائية للمسؤول [١]وقد كفلت جل الدساتير هذا الحق [٢] خاصة في ظل التطور التكنولوجي والمعلوماتي الذي أظهر تعرض هذا الحق الى العديد من المخاطر.

- **المطلب الأول:** المقصود بالبيانات الشخصية والاهتمامات التشريعية بها.
- **المطلب الثاني:** خصوصية البيانات الرقمية ومخاطرها

---

(١) ينظر: يونس عرب موسوعة القانون وتقنية المعلومات، قانون الكومبيوتر، منشورات اتحاد المعارف العربية، طبعة أولى، ٢٠٠١، ص ١٦٦.

(٢) ومن هذه الدساتير الدستور المصري لعام ٢٠١٤ في مادته ٥٧ على" للحياة الخاصة حرمة وهي مصونة لا تمس وللمراسلات البريدية والبرقية والإلكترونية والمحادثات الهاتفية وغيرها من وسائل الاتصال، حرمة وسريتها مكفولة ولا يجوز مصادرتها أو الاطلاع عليها أو تتبعها إلا بأمر قضائي مسبب ولمدة محددة وفى الأحوال التي يبينها القانون كما تلتزم الدولة بحماية حق المواطنين في استخدام رسائل الاتصال العامة بكافة أشكالها ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها بشكل تعسفي وينظم القانون ذلك".

المطلب الأول

المقصود بالبيانات الشخصية والاهتمامات التشريعية بها.

بعد تطور وسائل تقنية المعلومات الحديثة وبيان خطورتها على حرمة الأمن الشخصي للحياة الخاصة بات من الضروري العمل على توفير حماية حقيقية واضحة ومحددة تنتج من تضافر الجهود الدولية والمحلية لحماية هذا الحق وسن وتطوير تشريع قانوني يهدف إلى حماية تشريعية مدنية وجنائية ذات أطر محددة لهذا الحق وهو ما يستدعي الوقوف على تعريف محدد للمقصود من البيانات الشخصية.

- **التعريف الاصطلاحي:** " الحق في أن ينفرد الشخص في التحكم بالمعلومات التي تخصه مثل الاسم وغيرها من المعلومات التي تأخذ شكل بيان وثيق الصلة بكل شخص طبيعي" [1] وعليه تكون البيانات

(١) د. منى الأشقر جبور ومحمود جبور "البيانات الشخصية والقوانين العربية الأمنية وحقوق أفراده"، المركز العربي للبحوث القانونية والقضائية، الطبعة الأولى، بيروت، لبنان، عام ٢٠١٨، ص ٧٢-٨٩. والرجوع إلى طارق عثمان، الحماية الجنائية للحياة الخاصة عبر الإنترنت، رسالة ماجستير سنة= =٢٠٠٦-٢٠٠٧، ص ١٤-١٨، د. حمد أحمد المعداوي بحث بعنوان "حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي" نُشر في مجلة كلية الشريعة والقانون بطنطا، العدد ٣٣، الجزء الرابع، عام ٢٠١٨، ص ١٩٤٢-١٩٥٨، الموقع الإلكتروني:
https://mksq.journals.ekb.eg/article_30623_1ab2f80af612aa4568dbf6239b535ac2.pd
وينظر: بارق منتظر عبد الوهاب، جريمة انتهاك الخصوصية عبر الوسائل الالكترونية التشريع الأردني دراسة مقارنة، رسالة ماجستير مقدمة لكلية الحقوق جامعة الشرق الاوسط، ٢٠١٧، ص ١٢-٣٥.

الشخصية هي كل معلومة أو صورة أو صوت متعلق بشخص معروف أو قابل للتعرف عليه بصورة مباشرة أو غير مباشرة بالرجوع لعناصر تميزه عن غيره من الأشخاص سواء كانت نفسية او بدنية أو جينية او اقتصادية او ثقافية أو اجتماعية. [1]

- **التعريف الفقهي:** " البيانات الشخصية هي المعلومات التي يمكن من خلالها الاستدلال على هوية شخص ما كاسمه والمعلومات التي تشكل جزء من الحياة السرية للفرد والتي يضار بها صاحبها حال إفشائها" وتناولت تعريف البيانات الشخصية جهود فقهية[2] ويُعتبر الفقيه آلن ويستون من أوائل الفقهاء الأمريكيين الذين اهتموا بحماية البيانات الشخصية. في عام ١٩٦٧، عرّف في مؤلفه "الخصوصية والحرية" خصوصية البيانات بأنها "حق الفرد في تحديد متى وكيف، وإلى أي مدى تصل بياناته الخاصة إلى الآخرين" ،أما الفقيه ميلر، فقد عرّف الخصوصية في مؤلفه عام ١٩٧١ بعنوان "الاعتداء على الخصوصية" بأنها "قدرة الفرد على التحكم في تدفق المعلومات المتعلقة به"، مما يعني حق الفرد في منع الآخرين من الاطلاع على أو التصرف في المعلومات المتعلقة بحياته الخاصة [3] ، في السياق نفسه، عرّف المشرع المصري

(١) ينظر د. هشام فريد رستم قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، ١٩٩٢، ص ١٨٢.

(٢)أنظر حسام الدين الأهواني. الحق في احترام الحياة الخاصة دراسة مقارنة، دار النهضة العربية، القاهرة، ١٩٧٨، ص ٦١

(٣) شلواح ميرة، بشيرى كهينة، "المسؤولية المدنية عن انتهاك حق الخصوصية في المجال الرقمي"، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة – بجاية، ٢٠١٩-٢٠٢٠، ص. ١٠.

البيانات الشخصية في المادة الأولى من الفصل الأول من قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، بأنها "أي بيانات تتعلق بشخص طبيعي محدد أو يمكن تحديده بشكل مباشر أو غير مباشر، من خلال الربط بين هذه البيانات وأي بيانات أخرى، مثل الاسم أو الصوت أو الصورة، أو رقم تعريف أو محدد للهوية عبر الإنترنت، أو أي بيانات تحدد الهوية النفسية أو الصحية أو الاقتصادية أو الثقافية أو الاجتماعية "، واتجه البعض إلى تعريف البيانات الشخصية: بأنها كل بيان من شأنه أن يؤدي إلى معرفة المستخدم على وجه التحديد، أو يجعله قابلاً للتعرف عليه بصفة مباشرة أو غير مباشرة، ويشمل ذلك –دون حصر– الأسماء، وأرقام الهويات الشخصية، والعناوين، وأرقام التواصل، وأرقام الرُّخص والسجلات والممتلكات الشخصية، وأرقام الحسابات البنكية والبطاقات الائتمانية، وصور المستخدم الثابتة أو المتحركة، وغير ذلك من البيانات ذات الطابع الشخصي[1].

ووفقًا لتعريفها في المادة ٤/١ من اللائحة الأوروبية لحماية البيانات الشخصية، تُعرف البيانات الشخصية بأنها: "أي معلومات تتعلق بشخص طبيعي يمكن تحديده بشكل مباشر أو غير مباشر، وخاصة من خلال الإشارة إلى عنصر أو أكثر من العناصر المميزة له، مثل: الاسم، الرقم التعريفي، بيانات الموقع، معرف الاتصال عبر الإنترنت، أو الخصائص الفسيولوجية، الوراثية، النفسية، الاقتصادية، الثقافية، أو الاجتماعية".

(١) انظر في هذا المعنى تعريف هيئة الاتصالات والفضاء والتقنية السعودية https://www.cst.gov.sa/ar/Digitalknowledge/Pages/personaldata.aspx

استنادًا إلى التعريفات السابقة، يمكننا أن نعرف البيانات الشخصية أو البيانات ذات الطابع الشخصي بأنها: "المعلومات المرتبطة بشخص طبيعي محدد أو قابل للتحديد بشكل ما من خلال الربط بينها وبين معرفات معينة مباشرة أو غير مباشرة ".

وقد أحسن المشرع عندما حدد أنماط البيانات الشخصية التي تخضع للحماية القانونية من خلال تقديم أمثلة توضح هذه البيانات، مما ساهم في جعل مفهوم البيانات الشخصية أكثر وضوحًا ودقة، وأتاح التعريف المرونة اللازمة لتشمل مختلف أنواع البيانات الشخصية.

كما يتبين من النص السابق أن المشرع المصري قد قصر حماية البيانات الشخصية على الأشخاص الطبيعيين فقط، مستثنيًا الأشخاص الاعتباريين من نطاق هذه الحماية القانونية، إلا إذا كانت البيانات تتعلق بالأفراد الذين يمثلون الشخص الاعتباري [(١)].

وتقسم معرفات البيانات الشخصية إلى معرفات مباشرة إذا كانت تدل بشكل مباشر على هوية الشخص، كما توجد معرفات غير مباشرة:

١. **معرفات مباشرة:** الاسم، الصور الشخصية، البصمات، أرقام السجلات (الرقم القومي، رقم الجواز، رقم الرخصة، رقم الحساب البنكي) ، البطاقة الائتمانية، رقم التواصل، عنوان المنزل ، المعرف الرقمي (**IP**)، البريد الإلكتروني، بيانات صحية.

(١) سامح عبد الواحد التهامي، "ضوابط معالجة البيانات الشخصية: دراسة مقارنة بين القانون الفرنسي والقانون الكويتي"، مجلة القانون الكويتية العالمية، العدد ٩، السنة ٣، مارس ٢٠١٥، ص. ٤٠١.

٢. **معرفات غير مباشرة:** العمر، الجنس (ذكر، أنثى)، الدرجة العلمية، الراتب، الوظيفة، التواريخ المرتبطة (تاريخ الميلاد، الاشتراك، انتهاء خدمة)، اسم مستخدم مستعار، مكان الميلاد، مكان الوظيفة.

الهدف من تعريف البيانات الشخصية: هو توفير الحماية للحقوق والحريات للأشخاص الطبيعيين حال معالجة بياناتهم الشخصية لتشمل المعلومات المرتبطة بالتقنيات الحديثة والتي تحدد شخصا بشكل ما ولم تقتصر على المعلومات التي تحدد هوية الشخص بشكل مباشر فقط

والشخص الطبيعي المعني بالأمر هو كل شخص طبيعي تكون بياناته موضوعا للمعالجة الالكترونية مثل الموظف و ملفه الوظيفي، والمريض وملفه الطبي ولأجل تحقيق الحماية اللازمة اتسع مفهوم معالجة البيانات الشخصية حيث عرفته المادة ٢ (ب) من التوجيه الأوروبي " أي عملية أو مجموعة من العمليات المبرمة أو التي تستخدم الوسائل الآلية لكي تطبقها على البيانات الشخصية مثل الجمع أو التسجيل والتنظيم او الحفظ او التعديل أو التصميم أو الاستخراج أو الاسترجاع أو الاستخدام أو الإحالة عن طريق الارسال او النشر او أي شكل آخر من الأشكال المتاحة مثل التقريب أو الربط البيني او القفل أو المسح أو التدمير " ومما تجدر الإشارة إليه أن فرنسا أول بلد تنشئ هيئة وطنية لحماية البيانات الشخصية [١]

وفيما يتعلق بأنواع البيانات الشخصية، يمكن تقسيمها إلى نوعين:

١. **البيانات الشخصية العادية:** وهي المعلومات التي تتعلق بالفرد ولا يمانع من اطلاع الآخرين عليها، ولا تعتبر معرفتها انتهاكًا لخصوصيته. من أمثلة هذه البيانات: الاسم، رقم الهاتف، وتاريخ الميلاد.

(١) ينظر: د. محمد أحمد المعداوي، المرجع السابق ص ١٩٥٨ وما بعدها.

٢. **البيانات الشخصية الحساسة:** وقد عرّفها المشرع المصري في المادة (١) من الفصل الأول من قانون حماية البيانات الشخصية بأنها "البيانات التي تكشف عن الصحة النفسية أو العقلية أو البدنية، أو البيانات المالية، أو الآراء السياسية، أو الحالة الأمنية، أو المعتقدات الدينية، أو البيانات الجينية، أو البيانات البيو مترية للشخص". وقد حظر القانون التعامل مع هذه البيانات إلا بعد الحصول على ترخيص من مركز حماية البيانات الشخصية، وموافقة الشخص المعني بشكل صريح وكتابي.

ويرى البعض أن البيانات الحساسة تمثل نوعًا خاصًا من البيانات الشخصية ذات نطاق محدود. ويعود سبب حظر جمع هذه البيانات أو تداولها أو معالجتها إلى ارتباطها الوثيق بحق الفرد في خصوصية حياته. هذا الحق تم الاعتراف به في الدساتير الوطنية وكذلك في المعاهدات والمواثيق الدولية[١] .

الاهتمامات التشريعية في حماية الخصوصية وتعريفها:

اهتمت العديد من التشريعات في وضع تعريف الخصوصية والبيانات الشخصية:

المشرع التونسي: أصدر قانون رقم ٦٣ لسنة ٢٠٠٤ الخاص بحماية المعطيات والبيانات الشخصية والذي بموجبه يحظر قيام أي شخص بجمع معلومات يكون من شأنها تحديد هوية شخص معين باستثناء الغرض المشروع والمقترن بأذن الشخص المعني وأجاز القانون للهيئة الوطنية

(١) مادة ٩٢ من الدستور المصري لعام ٢٠١٤، والمادة ١٢ من الإعلان العالمي لحقوق الإنسان، والمادة ١٧ من العهد الدولي الخاص بالحقوق المدنية والسياسية.

لحماية المعطيات الشخصية الحصول على هذه البيانات واشترط أن يكون الغرض من جمع البيانات هو المصلحة أو الضرورة او الأغراض العلمية.

المشرع المغربي: في عام ٢٠٠٩ أصدر قانون حماية الأشخاص تجاه معالجة المعطيات ذات الطابع الشخصي لغرض حماية سرية المعطيات والبيانات الشخصية باتباع إجراءات تنظيمية وتقنية ملائمة لحماية المعطيات ذات الطابع الشخصي، إضافة لحمايتها من أشكال المعالجة غير المشروعة،

المشرع العماني: في قانون المعاملات الالكترونية نص في المادة ٤٣ منه على "يجوز لأية جهة حكومية أو مقدم خدمات تصديق أن يجمع بيانات شخصية مباشرة من الشخص الذي تجمع عنه البيانات أو من غيره بعد الموافقة الصريحة لهذا الشخص، وذلك فقط لأغراض إصدار شهادة أو المحافظة عليها أو تسهيل ذلك. ولا يجوز جمع البيانات أو معالجتها أو استخدامها لأي غرض آخر دون الموافقة الصريحة للشخص المجموعة عنه البيانات.

واستثناء من الفقرة السابقة يكون الحصول على البيانات الشخصية أو الإفصاح عنها أو توفيرها أو معالجتها مشروعا في الحالات الآتية:

أ- إذا كانت ضرورية لغرض منع أو كشف جريمة بناء على طلب رسمي من جهات التحقيق.

ب- إذا كانت مطلوبة أو مصرحا بها بموجب أي قانون أو كان ذلك بقرار من المحكمة.

ج- إذا كانت البيانات ضرورية لتقدير أو تحصيل أية ضريبة أو رسوم.

د - إذا كانت المعالجة ضرورية لحماية مصلحة حيوية للشخص المجموعة

عنه البيانات." [١]

المشرع المصري: عرف القانون المصري لحماية خصوصية البيانات ١٥١ لسنة ٢٠٢٠ م مادة (١) منه بأنها: "البيانات الشخصية: أي بيانات متعلقة بشخص طبيعي محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخرى كالاسم، أو الصوت، أو الصورة، أو رقم تعريفي، أو محدد للهوية عبر الإنترنت، أو أي بيانات تحدد الهوية النفسية، أو الصحية، أو الاقتصادية، أو الثقافية، أو الاجتماعية" ، وقد أولى المشرع اهتمامًا خاصًا بتنظيم التعامل مع البيانات الشخصية، وخاصة تلك الحساسة، حيث فرض عليها مستوى أعلى من الحماية مقارنة بالبيانات الشخصية الأخرى. وقد حدد المشرع بشكل حصري ما يمكن اعتباره بيانات حساسة في المادة الأولى من القانون. فعرف البيانات الشخصية الحساسة بأنها: " البيانات التي تفصح عن الصحة النفسية أو العقلية أو البدنية أو الجينية، أو بيانات القياسات الحيوية "البيو مترية" أو البيانات المالية أو المعتقدات الدينية أو الآراء السياسية أو الحالة الأمنية، وفي جميع الأحوال تعد بيانات الأطفال من البيانات الشخصية الحساسة" واستخدم المشرع المصري مصطلح "البيانات الشخصية الحساسة" للإشارة إلى فئة معينة من البيانات، وهو نفس المصطلح الذي اعتمده المشرع البحريني في القانون رقم ٣٠ لسنة ٢٠١٨ المتعلق بحماية البيانات الشخصية. وعلى النقيض، استخدم المشرع القطري مصطلح "البيانات الخاصة" في القانون رقم ١٣ لسنة ٢٠١٦. ورغم أن كلا المصطلحين يمكن أن يشيرا إلى هذه الفئة من البيانات الشخصية، إلا أن

(١) مرسوم سلطاني رقم ٦٩ / ٢٠٠٨ بإصدار قانون المعاملات الإلكترونية مادة ٤٣.

مصطلح "البيانات الشخصية الحساسة" يعد أكثر توافقًا وملاءمة لطبيعة هذه البيانات، نظرًا لأنها تمس حقوق وحريات الأفراد، والإفصاح عنها أو إساءة استخدامها قد يؤدي إلى أضرار جسيمة لهم، وعلى الرغم من أهمية تحديد هذه البيانات الحساسة بدقة، إلا أن المشرع المصري لم يوضح المعاني المقصودة بالمصطلحات المستخدمة في تعريف البيانات الحساسة، مما تركها في حالة من العمومية. وهذا قد يثير العديد من المشكلات عند تطبيق هذه المادة. كما أن تنوع مجالات البيانات الحساسة، سواء كانت مرتبطة بالحالة الصحية أو المالية أو التوجهات الدينية والسياسية، يجعل من الضروري تحديد المعاني المقصودة بالمصطلحات الواردة في التعريف بشكل دقيق [١]

(١) تناولت لائحة الاتحاد الأوروبي العامة لحماية البيانات ((GDPR٦٧٩ / ٢٠١٦ (EU's General Data Protection Regulation)) البيانات الشخصية الحساسة بالتنظيم وذكرت في المادة التاسعةُ مضمون هذه الفئة بأنها تلك البيانات التي تفصح عن الأصل العرقي، الآراء السياسية، المعتقدات الدينية أو الفلسفية، عضوية الاتحادات التجارية، البيانات الجينية والبيو مترية التي تستخدم بغرض تمييز الشخص الطبيعي، والبيانات الصحية والبيانات المرتبطة بالحياة الجنسية والميول الجنسية. ولتوضيح المقصود بالبيانات الجينية والبيو مترية والبيانات الصحية، ذكرت اللائحة في المادة الرابعة فقرة ١٣ تعريف البيانات الجينية بأنها البيانات الشخصية المرتبطة بصفات الشخص الطبيعي الجينية الموروثة أو المكتسبة والتي تعطي معلومات مميزة وفريدة عن صحته والتي تنتج عن تحليل العينات البيولوجية من الشخص الطبيعي المعني. وفي الفقرة ١٤ عرفت البيانات البيو مترية بأنها البيانات الشخصية الناتجة عن المعالجة الفنية للمواصفات الجسدية والفسيولوجية والسلوكية للشخص الطبيعي والتي تؤكد تميز هذا الشخص مثل صورة الوجه والبصمات. وفي الفقرة ١٥ عرفت البيانات الصحية بأنها تلك المرتبطة =

عند مقارنة التعريف الذي قدمه المشرع المصري بالتعريفات الواردة في لائحة الاتحاد الأوروبي، يمكننا أن نستنتج أنه رغم وجود توافق واضح في النطاق والمضمون، إلا أن التعريف الموجود في اللائحة الأوروبية يتميز بأنه أكثر دقة ووضوحًا، خاصة عندما يتعلق الأمر بالمصطلحات الفنية التي تحتاج إلى مزيد من التفسير فيما يخص البيانات الجينية أو البيو مترية. في حين أن المشرع المصري لم يقدم تعريفًا محددًا، بل ترك الأمر للفهم الدارج لهذه البيانات.

وفي شأن الحماية القانونية للخصوصية الرقمية: يسبق قانون حماية خصوصية البيانات ١٥١ لسنة ٢٠٢٠ م ما نص عليه في الدستور المصري من حماية حيث حظت البيانات الشخصية في المادة ٥٧منه بحماية باعتبارها حقاً اساسياً من حقوق الإنسان المرتبطة بحرمة الحياة الخاصة كما في التشريعات المصرية نصوصاً تعاقب على إفشاء البيانات الشخصية بالحبس لمدة لا تقل عن ستة أشهر مثل الأطباء المؤتمنون ببعض البيانات الشخصية بحكم عملهم أو إفشاء البيانات من قبل موظف مؤتمن مما يجعله مسؤولاً أمام القانون وفق ما نصت عليه المادة ٩ من قانون ٢٦٠ لسنة ١٩٦٠ المعدل بالقانون رقم ١٥٨ لسنة ١٩٨٠ على سرية

=

بالصحة الجسدية أو العقلية للشخص الطبيعي.. راجع في هذا: Article 4/13 states: 'genetic data' means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.

البيانات التي تحويها سجلات الأحوال المدنية كما يعاقب القانون كل من أفشى سراً أو بياناً من أسرار الصناعة او التجارة او اخل بسرية البيانات الإحصائية او البيانات الفردية أو غيرها مما يمكن الاطلاع عليه بمناسبة عمله و يشمل كذلك بحماية السرية بيانات العملاء البنكية ويمتد الأمر إلى ما بعد زوال العلاقة بين العميل والبنك ويشمل جميع الجهات والأشخاص ومنها التي تمتلك بموجب القانون سلطة الاطلاع على الأوراق أو البيانات المحظور افشاء سريتها وفقاً لأحكام قانون سرية الحسابات بالبنوك [١].

وتضمن الدستور العراقي: نص على أوجه عدة للخصوصية كالحق في سرية المراسلات وخصوصية المعلومات والحق في حرمة السكن ويقوم القضاء بتفسير النصوص الدستورية ففي حالة عدم النص على هذا الحق يعتبر مقرر ضمناً في النصوص الدستورية [٢].

كما أن الانضمام والمصادقة على الاتفاقيات الدولية التي اعترفت بهذا الحق تعد مصدراً له ، وبناءً عليه فان كل شخص له حق مراجعة المحاكم المختصة عند تعرضه لأي اعتداء على حق من حقوقه المتعلقة

---

(١) تتناول المادة ١٤٠ من القانون رقم ١٩٤ لسنة ٢٠٢٠، حيث خصص المشرع المصري الفصل التاسع من الباب الثالث لسرية الحسابات المصرفية. وقد نصت المادة ٢٣١ على فرض عقوبة الحبس لمدة لا تقل عن سنة، بالإضافة إلى غرامة لا تقل عن ٢٠٠ ألف جنيه، أو بإحدى هاتين العقوبتين، على من يخالف أحكام المادة ١٤٠ من هذا القانون.

(٢) ينظر : د. فوزية شريف، التطور التاريخي للحق في الخصوصية بين النصوص الدينية والأحكام الوصفية دراسة تحليلية، بحث منشور ومشارك في كتاب أعمال المؤتمر الدولي المحكم حول الخصوصية في مجتمع المعلوماتية، ٢٠١٩، في الفرع الثاني مفهوم الخصوصية بلا ترقيم، منشور على الموقع https://jilre.com

بالبيانات الشخصية الالكترونية وحقه في تعويض عادل جراء أي عمل غير مشروع أو خاطئ سبب له ضرر مادي أو معنوي متعلق ببياناته الشخصية بل وتوقيع العقوبة المناسبة للأفعال المجرمة والتي نص عليها قانون الجرائم الإلكترونية مثل معالجة البيانات الشخصية دون الحصول على ترخيص أو إفشاء البيانات الشخصية [١]، وقد جاء في قرار للمحكمة الدستورية في مصر" ثمة مناطق من الحياة الخاصة لكل فرد تمثل أغواراً لا يجوز النفاذ إليها وينبغي دوماً – ولاعتبار مشروع – ألا يقتحمها أحد ضماناً لسريتها وصوناً لحرمتها ودفعاً لمحاولة التلصص عليها أو اختلاس بعض جوانبها

(١) و قد قضى القضاء الفرنسي بإدانة مسؤول مؤسسة بنكية قام بنشر لائحة سوداء لزبائن البنك ليطلع عليها التجار ليتجنبوا التعامل معهم و ينتبهوا لهذا الخطر، كما اعتبرت الغرفة الجنائية بمحكمة النقض الفرنسية أن جمع البيانات الاسمية بما يمكن من التعرف على عناوين البريد الإلكتروني للأشخاص يعتبر تجميعاً غير مشروع للبيانات ولو كانت تلك البرامج لا تخزن العناوين التي تستغل لإرسال البريد المزعج (Spam) كما اعتبرت الغرفة الاجتماعية بمحكمة النقض الفرنسية أن الأجير الذي يقوم دون إذن المشغل بتشفير الحاسوب (cryptage) تلافياً لاطلاع الغير على ما يتضمنه الحاسوب المعد للعمل من مسائل خاصة مرتكب خطأ جسيماً . يبرر فصله ، كما اعتبرت من حق المحكمة إجراء معاينة على الحاسوب المسلم من المشغل للأجير الذي يعمل عليه لغرض الاطلاع فيما إذا كان الأجير يقوم بتبادل المراسلة عن طريق بريده الالكتروني مع أشخاص يتهمهم المشغل= =بالمنافسة طالما أن المعاينة تمت على يد عون قضائي بمحضر الأجير وإن ادعاء الاجير بالحياة الخاصة لا يمنع في حد ذاته إجراء التحقيق المشروع في القضية بما يضمن الحقوق لكل أطراف الخصومة" مشار إليه في د. عبد المجيد غمجيه، الحماية القضائية للمعطيات الشخصية، المعهد العالي للقضاء، منشور على الموقع http://www.ism.ma/basic/web/pdf/docetude/autre/autre2.pdf

وبوجه خاص من خلال الوسائل العلمية الحديثة التي تبلغ تطورها حداً مذهلاً "[1] هذا وعرفتها الاتفاقية الأوربية رقم ١٠٨ الصادرة عن المجلس الأوروبي بالمادة ٢/أ) بأن "المعطيات ذات الطابع الشخصي: هي كل المعلومات المتعلقة بشخص طبيعي معرف او قابل للتعرف عليه" والكثير من الدول قد أخذت بهذا الاتجاه في تشريعاتها ومنها العراق، وهناك من يعرفها باتجاهات وميول الشخص السياسية أو المدنية أو تعاملاته المالية ومعلوماته الصحية ،كما أولت لائحة الاتحاد الأوروبي اهتمامًا خاصًا بتنظيم قواعد التعامل مع البيانات الحساسة، حيث اشترطت تطبيق معايير حماية تتجاوز تلك المقررة للبيانات الشخصية الأخرى. وقد اعتمدت في هذا السياق على نهج وقائي يتضمن تنظيم الحقوق والالتزامات والإجراءات المرتبطة بعمليات المعالجة، كما نصت على عقوبات في حال عدم الالتزام بهذه القواعد.

تعقيب: يمكن القول بأن حماية خصوصية المعلومات الرقمية هي حماية البيانات بمعنى مواجهة الاعتداءات على البيانات الشخصية والخصوصية على إطلاقها تشمل خصوصية الاتصالات وخصوصية المكان والمراسلات الالكترونية والعادية وخصوصية البيانات فكلها ترتبط بالحق في خصوصية البيانات الرقمية.

(١) ينظر: د. عبد المجيد غمجيه، المرجع السابق.

المطلب الثاني

خصوصية البيانات الرقمية ومخاطرها

يقصد خصوصية البيانات الرقمية: حق المستخدمين في حفظ سرية بيانات هويتهم أو سلوكهم أثناء استخدام الأنظمة الرقمية، بما لا يعيق قدرة الأنظمة على أداء وظائفها.

ولعل البيانات الشخصية التي تُعرِّف عنّا، كالاسم، والعنوان، ورقم الهوية؛ هي الأساس لحماية الخصوصية. لكن قد تتوسع هذه البيانات لتشمل أيضاً معلومات أكثر حساسية تتعلق بسلوكنا، وممارساتنا، وصحتنا، وأفكارنا، ومعتقداتنا، وحالتنا المادية، وعاداتنا الشرائية، ولقد صنّف الباحثون المعلومات المرتبطة بالخصوصية إلى خمسة أنواع ولها خصائص تميزها

أولاً: انواع خصوصية البيانات الرقمية (١):

١. **خصوصية الحالة الجسدية والعقلية:** تشمل الخصائص الجسدية للإنسان مثل البصمات والقياسات الحيوية، والحالة الصحية والجينوم بالإضافة للمشاعر والآراء والأفكار. وقد يؤدي انتهاكها إلى التمييز في فرص الحصول على عمل بناءً على الآراء مثلاً، أو التمييز في اختيار بوليصة التأمين الصحي بناءً على التاريخ المرضي للمستخدم أو أن تستخدم هذه المعلومات للابتزاز والملاحقة.

٢. **خصوصية الحياة الاجتماعية:** وتشمل محتويات منصات التواصل الاجتماعي والتفاعلات الاجتماعية والمحادثات الشخصية ويُسهّل انتهاك هذه البيانات، على سبيل المثال، الحالة الصحية أو النفسية، أو الاتجاهات والآراء السياسية.

(١) محمد أحمد المعداوي، المرجع السابق ، ١٩٥٠ وما يليها.

٣. **خصوصية السلوك والأفعال:** وهي العادات، والهوايات، والأنماط الشرائية، عادة هذه المعلومات، عند تسريبها تستغل لأغراض الدعاية الموجهة.

٤. **خصوصية الوسائط:** وهي الصور، أو المقاطع المرئية والمقاطع الصوتية الخاصة بأي إنسان والدوائر التلفزيونية المغلقة ولقطات الكاميرات التي (تم التقاطها عن قصد أو عن غير قصد) وتعتبر إعادة التوزيع أو إنشاء هذه الوسائط المتعلقة بالأفراد أو نشرها دون موافقة أصحابها انتهاك لخصوصية المعنيين.

٥. **خصوصية الموقع الجغرافي:** وهي الإحداثيات الجغرافية للمواقع، وتوقيت ومدة زيارة هذه المواقع والتي قد يؤدي انتهاك الخصوصية فيها إلى كشف عناوين إقامة وعمل المستخدمين أو التعدي على أنواع الخصوصيات الأخرى.

هذه الأنواع من الخصوصية هي عرضة للانتهاك في العصر الحالي مع التطور التقني وانتشار انظمة الذكاء الاصطناعي بشكل مختلف في تعديل الصور والفيديوهات والبيانات.

ثانياً: الخصائص التقنية الواجب توافرها في خصوصية البيانات الرقمية:

تعرف الأدبيات العلمية والقانونية بعض الخصائص أو الأهداف المرجوة من التقنيات التي تتعامل مع البيانات مثل:

١. إخفاء الهوية بحيث لا يمكن تحديد هوية فرد من ضمن بيانات لمجموعة من الأشخاص.

٢. استخدام الأسماء المستعارة، وتعني الاستعاضة عن البيانات التعريفية (رقم الهوية – البريد الالكتروني) واستبدالها برموز وأرقام عشوائية، مما يسمح للنظام بالتعرف على المستخدم دون كشف هويته.

٣. عدم القدرة على الربط لمن لا يمتلك البيانات أن يربط بين حدثين قام بهما نفس المستخدم، كما لا يمكنه ربط أي حدث بالمستخدم.

٤. السرية وهي من أساسيات أمن المعلومات وليس خصوصيتها، إلا أنها متطلب أساسي لحماية الخصوصية وتعني منع وصول أي طرف آخر للمعلومات الخاصة بالأفراد.

ثالثاً: تقنيات تعزيز الخصوصية:

تقنيات تعزيز الخصوصية تهدف لتحقيق كل أو بعض خصائص التقنية الرقمية، باستخدام الوسائل تقنية أو المنهجية. وقد شهدت هذه التقنيات قفزات بظهور العديد من برامج حماية خصوصية الأفراد مثل متصفحات **Tor** و **Brave** التي اعتمدت على أساسيات منها.

أ. اعتماد الخصوصية كمتطلب أثناء تصميم البرمجيات: بحيث تبني أنظمة تحمي خصوصية المستخدم. وهذه المنهجية تستند على الالتزام ب

- مبدأ اعتماد الحد الأدنى من البيانات الشخصية التي يجمعها ويحتاجها النظام.
- مبدأ الشفافية وتعني إبلاغ المستخدم عن مبررات الحاجة إلى هذه البيانات، وكيفية استخدامها حصرياً.

وتتعزز هذه المبادئ بوجود قوانين حماية بيانات عصرية مثل القانون الأوروبي لحماية البيانات(**GRPR**) ، [١] الذي أجبر **WhatsApp** مثلاً

(١)"اللائحة العامة لحماية البيانات" (General Data Protection Regulation). هذه اللائحة هي إطار قانوني صادر عن الاتحاد الأوروبي يهدف إلى حماية خصوصية البيانات الشخصية للمواطنين وضمان أمان البيانات التي يتم جمعها ومعالجتها من قبل الشركات والمؤسسات.

على استثناء الأوروبيين من التحديث المثير للجدل، لتعارضه الواضح مع القانون.

ب. تقنيات التشفير: لتحويل البيانات إلى نصوص غير مفهومة باستخدام اساسيات رياضية للبيانات وبعض خوارزميات التشفير، بحيث تصبح القدرة على استعادة البيانات معدومة للأطراف التي لا تمتلك مفاتيح التشفير [١].

ج. تقنيات إخفاء البيانات التعريفية: تعمد هذه التقنيات إلى عدم اظهار البيانات الدالة على هويات الأفراد من مجموع البيانات. وتستعمل هذه الأساليب عند نشر بيانات التقارير الإحصائية.

رابعاً: مخاطر التي تهدد خصوصية البيانات الرقمية:

هناك العديد من الأسباب التي تجعل حماية الخصوصية والبيانات الشخصية على الإنترنت أمرًا مهمًا في ظل التطور التقني مما يهددها من استخدام البيانات الشخصية

(١) تم تطوير خوارزمية التشفير المتشاكل (Homomorphic Encryption) لتمكين إجراء عمليات معالجة أو حسابية على البيانات المشفرة مع الحفاظ على سريتها دون الحاجة إلى فك تشفيرها. وبالتالي، يمكن للجهات التي تجمع البيانات الشخصية تقديم خدماتها دون الحاجة إلى كشف هذه= =البيانات. كما يمكنها مشاركة هذه البيانات مع جهات أخرى غير موثوقة لتقديم خدماتها. على سبيل المثال، يمكن لشركة الهاتف تخزين نسخ مشفرة من بيانات الاتصالات الهاتفية لمستخدميها، وحساب قيمة فواتير المستخدمين لاحقًا دون الحاجة للاطلاع على تفاصيل هذه الاتصالات.

أ. **مخاطر تجميع البيانات الشخصية:** تُعرف عملية التجميع بأنها أي نشاط يتضمن جمع وترتيب عناصر البيانات الشخصية لشخص ما [1]فهي خطوة ضرورية في العديد من العمليات، حيث يتم إدراجها في بطاقات معلومات، ورقية أو إلكترونية وهذه المعالجة لا تخلو من المخاطر المتعلقة بانتهاك خصوصية البيانات المجمعة ويزداد هذا الخطر بسبب ربط الأجهزة المشتركة عبر شبكات عامة، مما يسهل تبادل البيانات الشخصية بينها ولعل من أشهر المخاطر التي تتعرض لها البيانات الشخصية إذا لم يتم حمايتها هي:

- سرقة بيانات الهوية: من خلال استخدام البيانات الشخصية للهوية وما يتبعه من فتح حسابات مصرفية أو بطاقات ائتمان باسم الشخص.
- الاحتيال: باستخدام البيانات الشخصية للاحتيال، محاولات إتمام صفقات الشراء من خلال بطاقات ائتمان مسروقة.
- الابتزاز: يمكن ايضاً انتهاك خصوصية البيانات الرقمية واستخدام البيانات الشخصية للابتزاز وتهديد الشخص بنشر معلومات خاصة عنه.
- الترويج غير المرغوب فيه: استخدام البيانات الشخصية للترويج للمنتجات أو الخدمات دون موافقة الشخص ولعل تطبيقات الذكاء الاصطناعي حالية سهلت هذا التهديد بشكل ملحوظ.

أشهر وسائل استخدام البيانات الشخصية على الإنترنت: تتمثل في إنشاء حساب على موقع ويب أو تطبيق أو تسجيل الدخول: يطلب الموقع أو التطبيق تقديم بعض البيانات الشخصية، مثل الاسم وعنوان بريد

(1)Cynthia chassigneux, L'encadrement juridique du traitement des données personnelles sur les sites de commerce en ligne, Thèse, Université Panthéon-Assas, Paris II, 2003, nº 278, p. 154.

الإلكتروني وكلمة المرور، التسوق عبر الإنترنت: يطلب موقع البيع الإلكتروني تقديم بعض البيانات الشخصية، مثل تفاصيل بطاقة الائتمان الخاصة بك ،وسائل التواصل الاجتماعي و مشاركة وسائل التواصل الاجتماعي بعض البيانات الشخصية، مثل اسم وصور وموقع المستخدمين ، استخدام الخدمات السحابية: تحفظ الخدمات السحابية بعض البيانات الشخصية، مثل الملفات التي تخزنها.

والاجدر بالأفراد أن يكونوا على دراية بكيفية استخدام بياناتهم الشخصية على الإنترنت، وحماية خصوصيتك الرقمية، فضلا عن التزام الدول بوضع حماية تشريعية تتناسب والتطور الهائل في هذا المجال التقني(١).

ب. مخاطر استخدام ومعالجة البيانات الشخصية: تشمل هذه المرحلة العديد من المخاطر، منها:

- **المخاطر المرتبطة باستخدام البيانات خلال عملية المعالجة (٢)ونتائجها:** حيث اعتبرت اللجنة الوطنية للمعلوماتية والحريات في فرنسا هذه المرحلة من البيانات الشخصية الحساسة، خاصة تلك المتعلقة بالهوس والفصام الذهني. وبالتالي، فإن معالجة البيانات الشخصية لأغراض

(١) محمد أحمد المعداوي، المرجع السابق ص ١٩٥٠ وما يليها.

(٢) عرف المشرع المصري المعالجة الإلكترونية في المادة (١) من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ بأنها: "أي عملية إلكترونية أو تقنية تتم بشكل كلي أو جزئي، تشمل الكتابة أو التجميع أو غيرها، باستخدام أي وسيلة من الوسائط أو الحاسبات أو الأجهزة الإلكترونية أو المغناطيسية أو الضوئية، أو أي تقنيات أو وسائط جديدة يتم تطويرها".

البحث العلمي، خصوصاً تلك المتعلقة بالأبحاث الجينية أو للأغراض الإحصائية.

- **المخاطر المرتبطة بأهداف عملية المعالجة:** استخدام البيانات المعالجة لتحقيق أهداف غير قانونية، بالإضافة إلى غموض الأهداف أو اتساع نطاقها أو تحديد أكثر من هدف من قبل المسؤول، مما يتيح مجالًا واسعًا لحدوث انتهاكات متعددة لخصوصية تلك البيانات.

ج. **مخاطر حوسبة البيانات الشخصية:** تُعرف حوسبة البيانات الشخصية بتقنية التعلم، حيث تتميز تطبيقاتها غالبًا بقدرتها على تكييف عملياتها وفقًا للبيانات التي تم جمعها. على سبيل المثال، في حالة المتجر متعدد الأقسام، يأخذ النظام في اعتباره المشتريات السابقة لترويج المنتجات المناسبة لنا وتعريفنا بمنتجات أخرى قد تهمنا. ومع انتشار عملية نقل البيانات الرقمية، ظهرت مشكلات أمنية عديدة، إذ سهلت هذه العملية عمليات التجسس الإلكتروني والقرصنة. وأصبحت شبكات الاتصال غير قادرة على ضمان الأمان المطلق أو السرية الكاملة للبيانات التي تُنقل عبرها [١].

د. **مخاطر تدفق البيانات عبر الإنترنت:** أدى تطور التكنولوجيا الرقمية إلى تدفق البيانات الشخصية للأفراد عبر الحدود، مما أتاح لهم فرصة مشاركة معلوماتهم الشخصية مع جهات داخلية أو خارجية. وهذا يعرض تلك البيانات للعديد من الانتهاكات، خاصة في الدول التي

(١) منى تركي الموسوى، الخصوصية المعلوماتية وأهميتها ومخاطر التقنيات الحديثة عليها، مجلة كلية بغداد للعلوم الاقتصادية، عدد ٢٩ خاص بمؤتمر الكلية، جامعة بغداد، ٢٠١٣، ص.٣١٢

تفتقر إلى مستويات عالية من الحماية. وقد دفع هذا الأمر المشرع المصري إلى حظر تداول البيانات الشخصية عبر الحدود. ومع ذلك، قد لا يكون هذا الحظر فعالاً في غياب التنسيق وضمان نقل البيانات ضمن إطار محكوم باتفاقات دولية تضمن مستوى مماثل أو أعلى من الحماية [١]

هـ. مخاطر استخدام البيانات في التسويق المباشر: البيانات الشخصية قيمة مادية في وقتنا المعاصر، ففيما يبدو أن البيانات المسجلة لدى العديد من الجهات مثل المصارف وشركات الهواتف المحمولة أصبحت تجارة رائجة تتداولها شركات التسويق، ضاربة عرض الحائط بمبادئ حماية خصوصية البيانات التي تنص عليها القوانين ويحميها حق دستوري

(١) في هذا السياق، أصدرت المحكمة العليا للاتحاد الأوروبي حكمًا بتاريخ ٦ أكتوبر ٢٠١٥ ببطلان اتفاق "الملاذ الآمن". وقد سمح هذا الاتفاق لشركة فيسبوك وبعض الشركات الأخرى مثل أمازون وجوجل بنقل كميات كبيرة من بيانات المستخدمين إلى خوادمها في الولايات المتحدة الأمريكية. وتبين لاحقًا أن أكثر من ٤٠٠٠ شركة قد استغلت هذا الاتفاق

.32ECLI, available at: http://curia.europa.eu/juris/document/document.jsf?docid=169195&docl ang=EN.

المبحث الثاني

انتهاك خصوصية البيانات الرقمية والمعالجة التشريعية

الخصوصية هي بتحكم الفرد في توقيت ومدي وظروف مشاركة بياناته الشخصية وتفاصيل حياته الخاصة مع الآخرين. وهذه الخصوصية حق يمارسه الفرد للحد من إطلاع الغير على تفاصيله الحياتية والتي قد تكون أفكاراً أو بيانات شخصية أو آراء أو عادات.

و"خصوصية البيانات الرقمية" هي وصف لحماية البيانات الالكترونية للفرد، والتي قد يتم نشرها وتداولها من خلال وسائط رقمية. وتتمثل هذه البيانات الشخصية في (البريد الإلكتروني، والحسابات البنكية، والصور الشخصية، ومعلومات عن العمل والمسكن..) هذه البيانات التي نستخدمها في نشاطنا وتفاعلنا على الإنترنت أثناء استخدامنا للحاسب الآلي أو التليفون المحمول أو أي من وسائل الاتصال الرقمي بشبكة الانترنت، مما جعل الخصوصية مهددة وأصبحت البيانات الشخصية مادة صالحة للانتهاك

المطلب الأول

التنظيم القانوني لحماية خصوصية البيانات الرقمية

إنً مشاركة البيانات الشخصية بصورة ما بعلم أو دون علم وهذه المشاركة لا تخلو من المخاطر واستغلال البيانات لذا لزم توفير حماية قانونية للبيانات الشخصية الرقمية وتحديث ما لا يتناسب مع تحديات التطور التكنولوجي والأتمتة الذكية لدخول المواقع الالكترونية عبر الانترنت التي لابد أن تكون محمية، ولعل أكثر من ١٦٠ دولة تشير في دساتيرها الحالية الى الحق في الخصوصية ولكن هذا الحق يختلف معناه من دولة إلى أخرى لأسباب تتعلق بالنظام الاجتماعي لها والتاريخ والثقافة والعادات

والتقاليد وغيرها وتبعا لذلك تختلف طريقة حماية هذا الحق وأن أول قانون تم إقراره لحماية البيانات الشخصية عام ١٩٧٠ من قبل ولاية هيس الاتحادية الألمانية ثم السويد وألمانيا وفرنسا [١].

(١) " أما اتفاقية ١٠٨ اتفاقية حماية الأشخاص تجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي التي تمت المصادقة عليها ١٩٨٠ و فتح باب التوقيع عليها ١٩٨١ و قد صادقت عليها الدول الاعضاء المجلس الأوروبي ال ٤٧ منذ اعتمادها و قد أدت دورا مهما في اعتماد أول قانون لحماية البيانات في أوروبا، وقد اضفى الاتحاد الأوربي من خلال الضوابط المنصوص عليها في المادة ٧ و ٨ من ميثاق الحقوق الأساسية للاتحاد الأوروبي حماية البيانات الشخصية باشتراط النزاهة في معالجة البيانات إضافة لتمكين الشخص المعني من الاطلاع على بياناته وتصحيحها إضافة لتولي الرقابة من قبل هيئة مستقلة ونص التوجيه الأوربي المرقم ٩٥/٤٦ في المادة ٦ على المبادئ الأساسية لحماية البيانات حيث تضمنت شروطاً لمعالجة البيانات الشخصية وهي (أ) . معالجة نزيهة وقانونية ب. جمعها لأغراض واضحة ومحددة مشروعة، وعدم معالجتها بطريقة أخرى غير متوافقة. تلك الأغراض ولا مع تعتبر المعالجة الزائدة للبيانات لأغراض تاريخية او علمية أو إحصائية غير متوافقة شريطة أن تقيم الدول الأعضاء الضمانات الأساسية المناسبة لحمايتها. أن تكون البيانات كافية ومتصلة بالغرض الذي تعالج أو جمعت من أجله وعدم زيادتها عنه، د. أن تكون دقيقة وأن يتم تحديثها عند الضرورة ويراعى اتخاذ كل ما هو معقول من خطوات لضمان مسح أو تصحيح البيانات غير الدقيقة او غير الكاملة مع الاخذ في الاعتبار الأغراض التي جمعت او التي يتم معالجتها من اجلها، هـ. الاحتفاظ بها في شكل يسمع صاحب البيانات لمدة لا تزيد عما هو ضروري للأغراض التي جمعت من أجلها أو يتم معالجتها من أجلها يتعين على الدول الأعضاء وضع الضمانات المناسبة للبيانات الشخصية المخزنة لفترات أطول للاستخدام التاريخي والإحصائي والعلمي "وبهذه الشروط يكون صاحب البيانات محمي وتوفر له ضمان معالجة سليمة لمعطياته الشخصية وحسب المادة ١٢ يحق =

أولاً: الحماية من التجسس والمراقبة الرقمية: يعني التجسس رصد أداء وأنشطة الأفراد وتفاعلهم في حياتهم اليومية، ولعل استخدام الإنترنت أحد هذه الأنشطة. وقد توّسع استخدم التجسس على الأفراد مع التطور التقني الذي مر به العالم وذلك طبقا للظروف التي تمر بها الدول وخاصة السياسية منها، وتلتزم الدول بحماية سرية المعلومات والبيانات الشخصية، وعلى الا نقوم بجمع أي معلومات شخصية إلا طواعية أو بإخطار لتقديمها من خلال قنوات التواصل الشرعية مثل الروابط الإلكترونية، التطبيقات الذكية، الاستبيانات، ونماذج التسجيل وغيرها. وأن هذه المعلومات لن تُستخدم لأي غرض آخر غير ما يتعلق بإنجاز ومعالجة الطلب المحدد لذلك، ولعل إقرار قانون خاص بحماية البيانات الشخصية يُظهر أن الدولة

=

لأصحاب البيانات معرفة السبب في معالجة بياناته من المتحكم بالمعالجة ومعرفة المنهج المستخدم في المعالجة إضافة لتصحيح الأخطاء في بياناتهم الشخصية وأشارت المادة ١٣ إلى حق الدولة في تقليص الالتزامات الواردة في ٦ و ١٠ و ١١ و ١٢ و ٢١ بسبب ضرورة النظام العام والأمن القومي او لمنع انتهاكات مهنية أو جنائية او لأسباب اقتصادية أو لأجل حماية حقوق وحريات الآخرين أو لحماية صاحب البيانات كما أشارت المادة ٢٢ من النظام الأوروبي على حق اللجوء للقضاء والمادة ٢٣ لحق المتضرر جراء تحليل بياناته بالتعويض، والمادة ٢٤ على الجزاء المترتب على الإخلال بالقواعد والمبادئ التوجيهية في مجال معالجة البيانات.." ينظر: منى تركي الموسوي والمدرس جان سيريال فضل الله، الخصوصية المعلوماتية وأهميتها و مخاطر التقنيات الحديثة عليها، مركز بحوث السوق وحماية المستهلك، بحث منشور بمجلة كلية بغداد للعلوم الاقتصادية العدد الخاص بمؤتمر الكلية، سنة ٢٠١٣، ص ١٧-٢٠ منشور على الموقع:
https://www.iasj.net/iasj/download/51b569f8c8bd04b7

تقدر خصوصية الأفراد وتوفر لهم البيئة المناسبة لتعزيز الإبداع. فالحماية القانونية التي توفرها الدولة تُعد من أبرز الضمانات التي تمنح الأفراد الشعور بالأمان والاطمئنان.

ثانياً: تشريعات حماية خصوصية البيانات الرقمية:

لا شك أن التشريعات التي تدافع عن الخصوصية تستند على تعريفها كقيمة هامة لدى الفرد والمجتمع وتختلف الأطر التشريعية لذلك من دولة لأخرى طبقا للمستجدات التي مرت بها كل دولة بشأن خصوصية البيانات الرقمية، والفلسفة التشريعية، وكيفية تطبيق القوانين والتحولات التي يمر بها المجتمع ومقدرة كل دولة على تبني تعديل قوانينها بناء على قضايا جديدة تكون خارج إطارها التشريعي ، هذه التشريعات والقوانين المعنية بحماية الخصوصية تهتم بحماية وسائط نقل المعلومات عن طريق الإنترنت أو الهواتف أو البريد، و تهتم أيضا بالحفاظ على سرية المعلومات المالية أو الصحية الخاصة بالأفراد وكذلك التي يتم تداولها من خلال التصفح والتواصل على الإنترنت، لذلك لابد أن تختلف وتتسع أنواع القوانين المختصة بالخصوصية في الفضاء الرقمي بين حماية البريد الإلكتروني، ومتابعة نشاط متصفح الإنترنت وفرض قيود على نشر بيانات التواصل الاجتماعي، . وفيما يلي نذكر أهم التشريعات وقوانين المعنية بحماية خصوصية البيانات الرقمية.

١. **قانون حماية البيانات:** هو القانون المعني بفرض الحماية التنظيمية على الشركات المقدمة لخدمات الإنترنت والتي تقوم بتخزين معلومات رقمية لعملائها من نشر هذه المعلومات أو مشاركتها مع أطراف أخرى دون إفادة من العميل.

٢. **قانون مراقبة الاتصالات:** هو القانون المعني بفرض الحماية التنظيمية لتُقيد مراقبة وسائل الاتصال، والتي تكون في مجال العمل أو الموجودة في الأماكن العامة أو حتى في المنزل.

٣. **قانون الحماية من جرائم الإنترنت:** يعنى بفرض الحماية التنظيمية لمنع الاستيلاء على الهوية أو سرقة البريد الإلكتروني وكل ما يخص حماية البيانات الشخصية التي يشاركها الفرد أثناء استخدامه للإنترنت.

ثالثاً: المحاولات الدولية في حماية خصوصية البيانات الرقمية:

المحاولات التشريعية: لقد تضمنت عدد من المعاهدات الدولية محاولات لحماية حق الفرد في الخصوصية، وضمان عدم تعرضه لتعسف أو تدخل غير قانوني في خصوصياته، أو شؤونه الخاصة وأن يحميه القانون من مثل هذا التدخل أو المساس [١] وقد ساهمت دول الاتحاد الأوروبي في سن تشريعات خاصة لحماية خصوصية البيانات الرقمية، ووضع بعض المعايير ضمن الاتفاقية الأوروبية لحقوق الإنسان والتي نصت في المادة الثامنة الخاصة بالخصوصية على:

"١. من حق أي شخص أن يحصل على احترام حياته الشخصية والعائلية بالإضافة لمنزله ومراسلاته.

٢. لا يحق للدولة التدخل في هذا الحق إلا بموجب القانون وما تمليه الضرورة في المجتمع الديمقراطي، وما يمس الأمن القومي أو السلامة العامة أو الاقتصادية للبلاد أو لمنع الفوضى وما قد يضر الصحة والآداب العامة أو لحماية حقوق وحريات الآخرين" [٢]

---

(١) العهد الدولي الخاص بالحقوق المدنية والسياسية– المادة ١٧

(2)Convention for the Protection of Human Rights and Fundamental Freedoms.

وقد أدي ذلك لتوسع مفهوم الخصوصية بالرغم من اختلافات تطبيق القانون من دولة لأخرى، فنجد لدى كل من اسبانيا وألمانيا أشد القوانين حزما، في حين أن إسبانيا أكثر الدول الأوروبية التي تسجل شكاوى ضد انتهاك حماية البيانات والأكثر في تحصيل الغرامات ضد انتهاكات البيانات الشخصية [١] وفي قارة آسيا، سنت سنغافورة في عام ٢٠١٢ تشريع قانون لحماية البيانات الشخصية يمنح حماية مدتها عشر سنوات بعد وفاة الشخص [٢]، وجاء قانون كوريا الجنوبية من أقوي التشريعات في آسيا حيث نصت أحد البنود القانون على حماية صورة وصوت الفرد [٣].

ويوجد العديد من دول أمريكا اللاتينية شرعت قوانين لحماية خصوصية الأفراد استرشاداً لتوجيهات دول الاتحاد الأوروبي بهدف فتح السوق التجارية معها. مثل الأرجنتين في عام ٢٠٠٠ أصدرت تشريعها الخاص لتسهيل التجارة بينها وبين دول الاتحاد الأوربي وكان التشريع مبني على معايير الاتحاد الأوروبي.

وفي الولايات المتحدة الأمريكية كانت قوانين الخصوصية بها غير مكتملة وتعاني من فقر تشريعي، فهناك قوانين تغطي البيانات المالية مثل الحسابات البنكية والعناوين [٤] ، وأخرى خاصة بالرعاية الصحية، و لديها تشريع يلزم المواقع التي تقوم بجمع معلومات عن الأطفال تحت سن ١٣ سنة بوضع سياسة خصوصية حول التحقق من موافقة الوالدين أو المسئول

(1) Data Protection Laws of the World, March 2013.
(2)Personal Data Protection Act 2012 – REPUBLIC OF SINGAPORE.
(3)FTC Staff Issues Privacy Report, Offers Framework for Consumers. Businesses and Policymakers.
(4)Gramm-Leach-Bliley Act – Bureau of Consumer Protection.

عن الطفل عند نشر الأطفال لبياناتهم [١]، وجدير بالذكر انه يوجد لديها أيضاً اسهامات غير محددة داخل الإطار تشريعي، مثل سياسة المتاجر الأمريكية الذاتية لحماية عملائها إلا أنها قد لا يقابلها أي عقوبة قانونية لحماية المستهلك وقد تبنت بعض المؤسسات صياغة مشاريع قوانين للخصوصية الرقمية طبقاً للتطورات التي تمر بها خصوصية البيانات الرقمية، مثل لجنة التجارة الفيدرالية الأمريكية **FTC** قدمت تقريراً يكشف عن أحقية المستهلكين في منع المواقع الإلكترونية من متابعة سلوكهم في استخدام الإنترنت [٢] ، وكانت النقطة المحورية فيه أنه يُقيّد برامج تصفح الإنترنت بإدراج وظيفة لعدم التتبع، كما يقترح بأن تكشف الكيانات التجارية عن الوضع الحالي للبيانات الشخصية التي قامت بجمعها ومع من قامت بمشاركتها ، وما تقدمت به المفوضية الأوروبية بتشريع لحماية البيانات والذي يجعل من حق الفرد أن يطلب من مقدمي خدمات الإنترنت بمسح بياناته الشخصية التي يمكن أن تظهر في محركات البحث وسمي التشريع بـ **Right to Be Forgotten**، والذي يسمح للمستخدمين أن يطالبوا شركات مثل جوجل ومنصة **x** وفيسبوك بحذف بياناتهم الخاصة ومنع ظهور هذه البيانات في محركات البحث لديها.

السبل الرقمية لحماية البيانات الشخصية:

لقد نتج أيضاً عن التطور التكنولوجي أشكال جديدة لحماية الخصوصية نظرا للانتهاكات المتزايدة التي تمارسها المواقع ومقدمو

(1) Children's Online Privacy Protection Act of 1998.
(2) FTC Staff Issues Privacy Report, Offers Framework for Consumers. Businesses and Policymakers – Federal Trade Commission.

الخدمات الرقمية ومن بين الآليات المستخدمة لحماية البيانات الشخصية بمختلف أشكالها سواء كانت نصية أو سمعية بصرية ولا شك من وجود العديد من وسائل الحماية الرقمية والإجراءات التي عنت بحماية خصوصية المستخدمين أو معلوماتهم الشخصية المتداولة عبر الوسائط الرقمية نذكر منها:

- **أمن البيانات الشخصية:** تُعتبر مسألة أمن البيانات الشخصية من أبرز التحديات القانونية المرتبطة بعملية المعالجة. تمر هذه العملية بعدة مراحل تتطلب توفير الحماية اللازمة لضمان عدم إفشاء سرية هذه البيانات. ومع ذلك، يزداد الأمر تعقيدًا يومًا بعد يوم، خاصة في ظل تزايد ظاهرة قرصنة المعلومات، مما يجعل مواجهة هذه التحديات أكثر صعوبة في ظل التطورات المستمرة في تقنيات التكنولوجيا الرقمية.

تناولت اللائحة الأوروبية هذه القضية في ثلاثة مواد (٣٢-٣٣-٣٤)، في محاولة لمواكبة التطورات السريعة في تكنولوجيا المعلومات، حيث أولت اهتمامًا كبيرًا بأمن وسرية البيانات. وقد نصت المادة (٣٢) على أن "المتحكم والمراقب والمتعاقد من الباطن يجب عليهم تنفيذ الإجراءات التقنية والتنظيمية المناسبة لضمان مستوى معين من الأمان يتناسب مع تلك المخاطر"، ومن بين هذه الإجراءات:

- استخدام الأسماء المستعارة وتشفير البيانات الشخصية.
- ضمان سلامة وسرية ومرونة أنظمة وخدمات المعالجة.
- توفير وسائل لاستعادة البيانات الشخصية والوصول إليها خلال فترة زمنية مناسبة في حال حدوث حادث مادي أو تقني.
- إجراء اختبارات دورية لفاعلية التدابير التقنية والتنظيمية وتحليلها وتقييمها لضمان أمن المعالجة.

كما حرص المشرع الأوروبي في المادة (٣٢) على الحفاظ على سرية وسلامة البيانات الشخصية وأمن المعالجة عند تقييم المستوى المناسب للأمان، مشددًا على ضرورة أخذ المخاطر الناتجة عن المعالجة بعين الاعتبار، والتي قد تشمل التلف أو الفقدان أو التغيير أو الكشف غير المصرح به عن البيانات، أو نقلها أو تخزينها أو معالجتها فالمشرع الأوروبي عمل على إنشاء نظام شامل لحماية أمن وسرية البيانات الشخصية، من خلال وضع تشريعات قانونية مناسبة، وتوفير الأدوات التقنية اللازمة، وتنظيم الإجراءات لضمان سلامة البيانات.

- **الحق في العزلة:** يعتبر تطور تقنيات التكنولوجيا الرقمية مفيدًا لحرية المعلومات، لكنه يثير مخاوف بشأن انتهاك خصوصية البيانات. مثل الإعلانات والرسائل الترويجية الواردة للشخص بناءً على الصورة النمطية المكونة عنه جراء دخوله المتكرر للمواقع المختلفة صورة من صور انتهاك الخصوصية عن طريق تقنية cookies[1]، تمثل هذه التقنية انتهاكا صارخا للبيانات الشخصية، فقد أدت حفظ وتخزين واستخدام البيانات المقدمة من محركات البحث مما أدى إلى المطالبة بحق الفرد العزلة أو نسيان بياناته ، حيث يسعى الأفراد للحصول على النسخة الأصلية من بياناتهم وإزالتها من السجلات. وفي ظل هذا التحدي، يتعين تحقيق توازن دقيق بين الحقوق والمصالح المتعارضة، مثل حماية البيانات الشخصية واحترام خصوصية الحياة الخاصة وحق الفرد في النسيان من جهة، وحرية المعلومات والإبداع الفني والأدبي والتاريخي من جهة أخرى.

(١) ملفات تعريف الارتباط

- **تطلب الموافقة المسبقة:** تستلزم العديد من التشريعات ولا سيما المشرع المصري بضرورة الحصول على موافقة صريحة من المستخدمين قبل جمع أو معالجة معلوماتهم الشخصية، وتكون هذه الموافقة مبنية على معلومات كافية حول استخدام المعلومات ووجهة استخدامها وأحسن المشرع المصري حين أعطى لشخص المعني بالبيانات الحق في التراجع عن الموافقة المسبقة التي أعطاها عند بدء عملية جمع ومعالجة بياناته الشخصية. ومع ذلك، يُنتقد المشرع المصري لشرطه بفرض مقابل مادي مقابل الخدمة المقدمة للشخص المعني من قبل المتحكم أو المعالج عند ممارسته لحقوقه، باستثناء الحق المتعلق بإخطار الشخص بأي خرق أو انتهاك لخصوصية بياناته الشخصية. وقد حدد مركز حماية البيانات الشخصية هذا المقابل بما يتجاوز عشرين ألف جنيه، وهو مبلغ مرتفع قد يعيق الشخص المعني عن ممارسة حقوقه التي يكفلها له القانون والدستور فيما يتعلق بحماية بياناته الشخصية. لذا، ينبغي على المركز عند تحديد أسعار الخدمات أن يأخذ في الاعتبار وضع رسوم تتناسب مع طبيعة البيانات الشخصية التي تحتاج إلى الحماية.
- **الحق في النسيان الرقمي:** أتاحت بعض القوانين للأفراد الحق في طلب حذف معلوماتهم الشخصية من الخوادم أو قواعد البيانات عندما تصبح هذه المعلومات غير ضرورية أو عندما الانسحاب من الموافقة، ويرى بعض الفقه المصري [١] أن هناك ارتباطًا وثيقًا بين الحق في النسيان

(١) أنظر: يونس عرب موسوعة القانون وتقنية المعلومات، قانون الكومبيوتر، منشورات اتحاد المعارف العربية، طبعة أولى، ٢٠٠١، ص ١٦٦.

الرقمي والخصوصية، إلا أن هذا لا يعني بالضرورة تلازمهما. فالحق في النسيان يُعتبر حقًا مستقلًا عن الحق في الخصوصية. فقد يتم الاحتفاظ بالبيانات لأسباب تتعلق بالمصلحة العامة، مما يؤدي إلى حماية تلك البيانات بموجب الحق في النسيان لفترة أطول من المدة المحددة لأغراض المعالجة، وبالتالي قد تخرج هذه البيانات عن نطاق الحماية المقررة بموجب الحق في الخصوصية. وهذا يعني أنه يمكن اعتبار الحقين مستقلين عن بعضهما البعض.

الحالات التي يحق فيها للشخص المعني بالبيانات ممارسة حقه في النسيان الرقمي هي:

وفقًا للمادة (٧) من اللائحة الأوروبية، يُمنح الشخص المعني حق النسيان، مما يتيح له إمكانية طلب محو بياناته الشخصية. ويتعين على المتحكم في البيانات تنفيذ هذا الطلب في أقرب وقت ممكن، شريطة أن ينطبق أحد الأسباب التالية:

١. لم تعد البيانات الشخصية ضرورية للأغراض التي تم جمعها من أجلها، أو تمت معالجتها بطرق أخرى.
٢. سحب الشخص المعني الموافقة المسبقة التي تم بموجبها معالجة البيانات، ولا يوجد أساس قانوني آخر يسمح بالمعالجة.
٣. عدم وجود أسباب مشروعة للمعالجة، أو في حالة معالجة البيانات الشخصية بشكل غير قانوني.
٤. ضرورة محو البيانات الشخصية للامتثال لالتزام قانوني منصوص عليه في قانون الاتحاد أو بموجب قانون الدولة العضو التي يخضع لها المتحكم.

٥. محو البيانات الشخصية كشرط للحصول على خدمات مجتمع المعلومات، إذا تم ذلك بشكل غير قانوني.

الاستثناءات المتعلقة بحق الأفراد في حذف بياناتهم وفقًا للائحة الأوروبية تشمل ما يلي:

١. المعالجة ضرورية للامتثال لالتزام قانوني يتطلب ذلك في مجالات العمل والضمان الاجتماعي أو بموجب قانون الحماية الاجتماعية أو اتفاقية جماعية.
٢. لأسباب تتعلق بالمصالح الحيوية للشخص المعني بالبيانات أو لشخص آخر، عندما يكون الشخص المعني غير قادر على إعطاء موافقته.
٣. لإنشاء الدعاوى القانونية أو ممارستها أو الدفاع عنها، أو عندما تتصرف المحاكم بصفتها القضائية.
٤. لأسباب تتعلق بالمصلحة العامة الجوهرية لقانون الاتحاد أو الدولة العضو.
٥. لأغراض الطب الوقائي أو المهني أو لإدارة أنظمة وخدمات الرعاية الصحية والاجتماعية.
٦. تتم المعالجة في إطار مشروع مع وجود ضمانات مناسبة من قبل مؤسسة أو هيئة غير ربحية، بشرط أن تتعلق المعالجة بأعضاء الهيئة أو الأشخاص المرتبطين بها بشكل منتظم، وألا يتم الكشف عن البيانات خارج الهيئة دون موافقة الأشخاص المعنيين.
٧. لأسباب تتعلق بالمصلحة العامة في مجال الصحة العامة، مثل الحماية من الأمراض الخطيرة أو ضمان معايير عالية لجودة الرعاية الصحية والمنتجات الطبية.

٨. معالجة البيانات لأغراض الأرشفة من أجل المصلحة العامة، أو لأغراض البحث العلمي أو التاريخي، أو لأغراض إحصائية وفقًا للمادة (١/٨٩).

المطلب الثاني

حماية خصوصية البيانات الرقمية في القانون المصري.

الحق في حماية أمن الحياة الخاصة أحد الحقوق المعترف بها وقد أظهر التطور إمكانية الاعتداء على هذا الحق ما لم يتم تنظيمه قانونا بتحديد كيفية استخدامه وآلية تنظيم تداول وتخزين ومعالجة البيانات الشخصية وتحديد المسؤولية المدنية أو الجنائية للمعتدي على البيانات الشخصية [١].

وقد كفل الدستور المصري هذا الحق [٢]، وهذا مبدأ معتبر على اختلاف تشريعات وقوانين الخصوصية بغرض أساسي هو السماح للأفراد بحرية التعبير والتفاعل بدون قلق أو رقابة من الاستغلال أو التشهير ويتبين

---

(١) يونس عرب ، المرجع السابق .

(٢) نصت المادة ٣ من الدستور المصري لعام٢٠١٤ المعدل ٢٠١٩" من القضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه على النحو الذي ينظمه (القانون" والمادة ٥٧ "للحياة الخاصة حرمة وهي مضمونة لا تمس والمراسلات البريدية والبرقية والإلكترونية والمحادثات الهاتفية وغيرها من وسائل الاتصال حرمة وسريتها مكفولة ولا تجوز مصادرتها أو الاطلاع عليها أو تتبعها إلا بأمر قضائي مسبب ولمدة محددة وفى الأحوال التي بينها القانون كما تلزم الدولة بحماية حق المواطنين في استخدام رسائل الاتصال العامة بكافة أشكالها ولا يجوز تعطيلها أو وقفها او حرمان المواطنين منها بشكل تعسفي وينظم القانون ذلك".

من الدستور المصري والدساتير المقارنة عدم النص صراحة على حماية الحق في خصوصية البيانات إنما وضع أساسا قانونيا لهذه الحماية تاركا المجال للتشريع الخاص وضع التنظيم القانوني المناسب لمعالجة هذه الضمانة وتحديد نطاقها ومصر شأنها ليس شأن دول كثيرة تأثرت خصوصية البيانات الرقمية فيها بالفراغ التشريعي الذي يخص قضايا الإنترنت وتداول المعلومات وعدم وضوح الأطر التي تحمي الحريات الرقمية بصفة عامة وخصوصية البيانات الرقمية بصفة خاصة فقد تضمن التشريع المصري قانون خاص لحماية خصوصية البيانات الرقمية، هو قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ بالإضافة إلى وجود بعض المواد الدستورية التي ذكرت الخصوصية، وتحدثت بصورة غير صريحة عن بعض الأنشطة الإلكترونية ولكن هل عالج القانون المعني الحماية المطلوبة للخصوصية الرقمية في مصر بالشكل الكافي ؟

أولا: المعالجة الدستورية لحماية خصوصية البيانات الرقمية.

عنى الدستور المصري ٢٠١٤ المعدل في ٢٠١٩ بحماية المواطنين الخاصة وحرمتها وسريتها وكفالتها وكذلك المراسلات المختلفة والمحادثات ووسائل الاتصال، وتظهر قيمة وأهمية الأمن الرقمي والحفاظ عليه في المادة ٣١ من الدستور المصري [١]، وكذلك المادة ٥٧ [٢]، والمادة٦٨ [١]

---

(١) المادة ٣١ من الدستور المصري " أمن الفضاء المعلوماتي جزء أساسي من منظومة الاقتصاد والأمن القومي، وتلتزم الدولة باتخاذ التدابير اللازمة للحفاظ عليه، على النحو الذي ينظمه القانون".

(٢) المادة ٥٧ من الدستور المصري ٢٠١٤ " " للحياة الخاصة حرمة، وهي مصونة لا تمس وللمراسلات البريدية، والبرقية، والإلكترونية، والمحادثات الهاتفية، وغيرها من وسائل الاتصال حرمة، وسريتها مكفولة، ولا تجوز مصادرتها، أو الاطلاع =

منه، وبالتالي أظهر النقاط التي قد تهدد هذا الأمان، من المستفيدين بشكل غير قانوني من البيانات الشخصية سواء بطريق مباشر أو غير مباشر بتبعيتها لكيانات تجارية وغيرها.

ثانياً: المعالجة التشريعية لحماية خصوصية البيانات الرقمية.

لقد أظهر المشرع المصري اهتمامًا كبيرًا في مواكبة التطورات التكنولوجية والمعلوماتية التي يشهدها العالم في العصر الحديث، من خلال إصدار مجموعة من التشريعات الضرورية لمواجهة هذا التقدم التقني في فضاء المعلومات ، ومن بين هذه التشريعات، قانون تنظيم الاتصالات رقم ١٠ لسنة ٢٠٠٣، الذي يهدف إلى تأمين نقل وتبادل المعلومات(٢) ،

=

عليها، أو رقابتها إلا بأمر قضائي مسبب، ولمدة محددة، وفى الأحوال التي يبينها القانون. كما تلتزم الدولة بحماية حق المواطنين في استخدام وسائل الاتصال العامة بكافة أشكالها، ولا يجوز تعطيلها أو وقفها أو حرمان المواطنين منها، بشكل تعسفي، وينظم القانون ذلك"

(١) المادة ٦٨ من الدستور المصري "المعلومات والبيانات والإحصاءات والوثائق الرسمية ملك للشعب، والإفصاح عنها من مصادرها المختلفة، حق تكفله الدولة لكل مواطن، وتلتزم الدولة بتوفيرها وإتاحتها للمواطنين بشفافية، وينظم القانون ضوابط الحصول عليها وإتاحتها وسريتها، وقواعد إيداعها وحفظها، والتظلم من رفض إعطائها، كما يحدد عقوبة حجب المعلومات أو إعطاء معلومات مغلوطة عمداً".

(٢) عرفت المادة الأولى من هذا القانون وسائل الاتصالات بأنها: "أي وسيلة تستخدم لإرسال أو استقبال الرموز أو الإشارات أو الرسائل أو الكتابات أو الصور أو الأصوات، بغض النظر عن طبيعتها، سواء كان الاتصال سلكياً أو لاسلكياً". وقد أقر المشرع في الباب السابع من هذا القانون مجموعة من العقوبات التي تُطبق في حالة التعرض أو الاعتداء على تلك الخدمات أو استغلالها بطرق غير قانونية.

بالإضافة إلى القانون رقم ١٥ لسنة ٢٠٠٤ المتعلق بتنظيم التوقيع الالكتروني وإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات، وذلك لضمان أمان معاملات الأفراد عبر شبكة الإنترنت بالإضافة إلى ذلك، أصدرت الوزارة المعنية بتكنولوجيا المعلومات والاتصالات العديد من القرارات التنظيمية بهدف تعزيز حماية تقنية المعلومات والاتصالات.

كما أنشأت مصر، بناءً على قرار مجلس الوزراء رقم ٢٢٥٩ لسنة ٢٠١٤، مجلسًا أعلى للأمن السيبراني، حيث تتولى مهمته وضع استراتيجية وطنية لمواجهة تحديات وأخطار والهجمات السيبرانية بالإشراف على تنفيذها وتحديثها بما يتماشى مع التطورات التقنية.

وفي ١٩ سبتمبر ٢٠١٤، أصدر السيد رئيس الجمهورية القرار رقم ٢٧٧ لسنة ٢٠١٤، الذي وافق فيه على انضمام مصر إلى الاتفاقية العربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، والتي تم توقيعها في القاهرة بتاريخ ٢١ ديسمبر ٢٠١٠.

وتم توقيع الاتفاقية العربية لمكافحة جرائم تقنية المعلومات في القاهرة بتاريخ ٢١ ديسمبر ٢٠١٠ [١]، مع التحفظ على شرط التصديق. تهدف هذه الاتفاقية إلى تعزيز التعاون بين الدول العربية في مجال مكافحة جرائم تقنية المعلومات، وذلك لحماية أمن الدول العربية ومصالحها وسلامة مجتمعاتها وأفرادها من مخاطر هذه الجرائم [٢].

(١) وقد وافقت مصر على الانضمام إليها بموجب قرار رئيس الجمهورية رقم ٢٧٦ لسنة ٢٠١٤ الصادر في ١٩ أغسطس ٢٠١٤، والذي نُشر في الجريدة الرسمية بالعدد ٤٦ بتاريخ ١٣ نوفمبر ٢٠١٤.

(٢) تُعتبر هذه الاتفاقية من أبرز الاتفاقيات العربية في مجال مكافحة الجريمة التقنية، =

ومن بين أحدث التطورات التشريعية لحماية المجال الرقمي وأهمها، يأتي القانون رقم ١٧٥ لسنة ٢٠١٨ المتعلق بمكافحة جرائم تقنية المعلومات، بالإضافة إلى لائحته التنفيذية رقم ١٦٩٩ لسنة ٢٠٢٠، يعالج هذا القانون الاطر الجنائية والاجرائية والعقابية المرتبطة بالانتهاكات الالكترونية يمنح هذا القانون الجديد الجهات المختصة في التحقيق صلاحية حجب المواقع الإلكترونية التي تنشر محتويات تشكل تهديدًا "لأمن البلاد أو اقتصادها". كما يحظر القانون "نشر معلومات تتعلق بتحركات الجيش أو الشرطة، أو الترويج لأفكار التنظيمات الإرهابية"، ويكلف رؤساء المحاكم الجنائية بالتحقيق والتفتيش لجمع الأدلة اللازمة لإثبات ارتكاب الجرائم التي تستوجب العقوبة وينص القانون أيضًا على أن الشركات المقدمة للخدمات أو مستخدمي الإنترنت الذين يقومون بزيارة المواقع المذكورة، سواء عن قصد أو "عن طريق الخطأ دون مبرر مقبول"، قد يواجهون عقوبات تصل إلى السجن وغرامة مالية [١].

=

حيث تسعى إلى منع هذه الجرائم والتحقيق فيها وملاحقة مرتكبيها، بما في ذلك الاعتداء على سلامة البيانات، وإساءة استخدام وسائل التقنية، والتزوير، والاحتيال، والإباحية، والاعتداء على خصوصية الأفراد.

(١) حاتم أحمد محمد بطيخ، دراسة تحليلية مقارنة لنصوص قانون مكافحة جرائم تقنية المعلومات الواردة في قانون مكافحة جرائم تقنية المعلومات المصري، رقم ١٧٥ لسنة ٢٠١٨. صفحة ٩. بنك المعرفة المصري.
https://jdl.journals.ekb.eg/article_191190_a30e591b0e0d147fc7926c2b98b33217.pdf

ويأتي قانون رقم ١٨٠ لسنة ٢٠١٨ بإصدار قانون تنظيم الصحافة والإعلام والمجلس الأعلى لتنظيم الإعلام في يونيو ٢٠١٨ وقد تم نشر المصادقة على القانون في الجريدة الرسمية، حيث تسري أحكامه على جميع الكيانات والمؤسسات والوسائل الصحفية والإعلامية والمواقع الإلكترونية.

كما جاءت نصوص قانونية جاءت نصت على حماية البيانات الشخصية لعملاء البنوك، والعاملين، والمرضى نصت عليها قوانين العمل، والبنوك، والأحوال الشخصية.

أما قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ فهو المعنى الأول بحماية الخصوصية محل الدراسة والذي نتناوله بشيء من التفصيل على النحو التالي:

في يوليو عام ٢٠٢٠ صدر قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠ والذي تسعى الدولة المصرية من خلاله إلى فرض سيطرتها على المجالات الرقمية وتداول البيانات، من خلال تحقيق المعايير الدولية في هذا المجال والضمانات الدستورية المقررة من قبل، وجميع القوانين بهدف ضمان الحقوق والحريات الشخصية وعدم استخدام البيانات بشكل غير قنوني من قبل السلطات أو غيرها.

تم إصدار هذا القانون بعد سلسلة من الجلسات والنقاشات التي استمرت لعدة أشهر لمناقشة مشروع القانون الذي قدمته الحكومة. ويتكون القانون من تسع وأربعين مادة، بالإضافة إلى سبع مواد تتعلق بالإصدار، موزعة على أربعة عشر فصلاً تتناول الجوانب المختلفة لتنظيم التعامل مع البيانات الشخصية. وقد اتبع المشرع المصري نهجين مختلفين لحماية البيانات الشخصية، حيث قام باستثناء بعض البيانات من الحماية التشريعية

المعلوماتية من جهة، وفرض حماية مشددة على بعض البيانات الأخرى من جهة أخرى.

فجاءت المادة الثالثة من مواد إصدار هذا القانون بالنص على " لا تسري أحكام القانون المرافق على ما يأتي:

١. البيانات الشخصية التي يحتفظ بها الأشخاص الطبيعيون للغير، ويتم معالجتها للاستخدام الشخصي.
٢. البيانات الشخصية التي تتم معالجتها بغرض الحصول على البيانات الإحصائية الرسمية أو تطبيقًا لنص قانوني.
٣. البيانات الشخصية التي تتم معالجتها حصرًا للأغراض الإعلامية بشرط أن تكون صحيحة ودقيقة، وألا تستخدم في أي أغراض أخري، وذلك دون الإخلال بالتشريعات المنظمة للصحافة والإعلام.
٤. البيانات الشخصية المتعلقة بمحاضر الضبط القضائي والتحقيقات والدعاوى القضائية.
٥. البيانات الشخصية لدى جهات الأمن القومي، وما تقدره لاعتبارات أخرى. ويجب على المركز، بناءً على طلب جهات الأمن القومي، إخطار المتحكم أو المعالج بتعديل أو محو أو عدم إظهار أو إتاحة أو تداول البيانات الشخصية، خلال مدة زمنية محددة، وفقًا لاعتبارات الأمن القومي، ويلتزم المتحكم أو المعالج بتنفيذ ما ورد بالإخطار خلال المدة الزمنية المحددة به.
٦. البيانات الشخصية لدى البنك المركزي المصري والجهات الخاضعة لرقابته وإشرافه، عدا شركات تحويل الأموال وشركات الصرافة، على أن يراعى في شأنهما القواعد المقررة من البنك المركزي المصري بشأن التعامل مع البيانات الشخصية."

يظهر من النص أنه تم استبعاد بيانات معينة من أحكام هذا القانون لأسباب واعتبارات متنوعة لم يحددها المشرع، رغم أنه يمكن استنتاجها من طبيعة هذه البيانات. ومن هذه البيانات: الاستخدام الشخصي، الأغراض الإحصائية الرسمية، تطبيق القانون، الإعلام ونشر المعرفة، العمل القضائي، الأمن القومي، والمعاملات المالية التي تخضع لإشراف البنك المركزي المصري وإن استبعاد هذه البيانات من تطبيق أحكام هذا القانون لا يعني أنها غير خاضعة لأي تنظيم قانوني، بل يعني أنها تخضع لأحكام قوانين أخرى تنظم هذا المجال نظرًا لخصوصيتها. وفق القاعدة القانونية التي تنص على أن الخاص يقيد العام على الجانب الاخر فرض المشرع حماية قانونية مشددة لفئة معينة من البيانات، والتي أطلق عليها "البيانات الحساسة"، فقد عرفها في المادة الأولى من القانون بأنها " البيانات التي تفصح عن الصحة النفسية أو العقلية أو البدنية أو الجينية، أو بيانات القياسات الحيوية "البيو مترية" أو البيانات المالية أو المعتقدات الدينية أو الآراء السياسية أو الحالة الأمنية، وفي جميع الأحوال تعد بيانات الأطفال من البيانات الشخصية الحساسة."

ونظم أحكامها في المادة ١٢ حيث ذكر" يحظر على المتحكم أو المعالج سواء كان شخصًا طبيعيا أو اعتباريًا جمع بيانات شخصية حساسة أو نقلها أو تخزينها أو حفظها أو معالجتها أو إتاحتها إلا بترخيص من المركز [١]. وفيما عدا الأحوال المصرح بها قانونًا، يلزم الحصول على

(١)مركز حماية البيانات الشخصية، نص المشرع في المادة ١٩ من القانون على إنشاء هيئة عامة اقتصادية تتبع الوزير المختص وتكون لها الشخصية الاعتبارية وتهدف إلى حماية البيانات الشخصية وتنظيم معالجتها وإتاحتها. نظم المشرع في الفصل =

موافقة كتابية صريحة من الشخص المعني. وفي حالة إجراء أي عملية مما ذكر تتعلق ببيانات الأطفال، يلزم موافقة ولي الأمر. ويجب ألا تكون مشاركة الطفل في لعبة أو مسابقة أو أي نشاط آخر مشروطة بتقديم بيانات شخصية للطفل تزيد على ما هو ضروري للمشاركة في ذلك. وذلك كله وفقًا للمعايير والضوابط التي تحددها اللائحة التنفيذية لهذا القانون".

ولقد قام المشرع بتحديد الأصل في البيانات الحساسة على أنه حظر التعامل معها بأي شكل من الأشكال. ومع ذلك، استثنى من ذلك إمكانية التعامل بعد الحصول على ترخيص من مركز حماية البيانات الشخصية وموافقة كتابية صريحة من الشخص المعني بالبيانات، أو في الحالات المصرح بها قانونًا. وتعود أسباب فرض حماية مشددة لهذه الفئة من البيانات إلى طبيعتها، حيث ترتبط ارتباطًا وثيقًا بحريات الأفراد، ويمكن أن تكشف عن هويتهم ونمط حياتهم، مما قد يهدد أمنهم وسلامتهم في حال تم انتهاك [١]هذه البيانات أو إساءة استخدامها. ومن الجدير بالذكر أن المشرع المصري اعتمد على فكرة الموافقة المسبقة كشرط لمشروعية معالجة البيانات الحساسة، حيث يجب أن تكون هذه الموافقة مكتوبة وصريحة، مما يجعلها بمثابة حصن إجرائي لحماية هذه البيانات من سوء الاستخدام [٢].

=

التاسع من القانون نشأة المركز تشكيله واختصاصاته وجميع المسائل الاخرى المرتبطة به في المواد من ١٩ حتى ٢٥.

(١) طارق جمعة السيد راشد، الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي، مجلة القانون والاقتصاد، العدد ٩٢، ٢٠١٩، ص.٢١٧.

(٢) طارق جمعة السيد راشد، الحماية القانونية للحق في خصوصية البيانات الجينية – دراسة تحليلية مقارنة، المجلة القانونية، مجلد ٨، العدد ١٢، ٢٠٢٠ ص ٣٩٧٥

اختتم المشرع نصوص هذا القانون بالفصل الرابع عشر، الذي خصصه للجرائم والعقوبات والجزاءات، حيث تضمن ١٤ مادة تتفاوت بحسب طبيعة المخالفة ومرتكبها، سواء كان مسؤول الحماية أو المتحكم أو المعالج أو أي شخص آخر. كما أتاح المشرع في المادة ٤٩ إمكانية الصلح مع المجني عليه، ونظم الإجراءات والآثار المترتبة على ذلك.

وعلى الرغم من أهمية هذا القانون وضرورة إصداره، إلا أنه تأخر كثيرًا حتى أصبح واقعًا. وقد سبقت مصر العديد من الدول العربية في إصدار قوانين لحماية البيانات الشخصية. حيث كانت تونس أول دولة عربية تنظم التعامل مع البيانات الشخصية من خلال قانون حماية المعطيات الشخصية رقم ٦٣ لسنة ٢٠٠٤، تلتها المغرب التي أصدرت قانون حماية المعطيات ذات الطابع الشخصي رقم ٠٨/٠٩ في عام ٢٠٠٩. كما أصدرت قطر قانون خصوصية البيانات الشخصية رقم ١٣ لسنة ٢٠١٦، والإمارات العربية المتحدة أصدرت قانون حماية البيانات الشخصية الفيدرالي رقم ٤٥ لسنة ٢٠٢١.

بعض الدول لم تصدر قوانين مستقلة لحماية البيانات الشخصية، بل أدخلتها ضمن قوانين أخرى، كما هو الحال في سلطنة عمان التي وضعت نصوصًا تنظم وتحمي البيانات الشخصية في قانون المعاملات الإلكترونية رقم ٦٩ لسنة ٢٠٠٧[١].

(١)الشيخ الحسين محمد يحي وسيد محمد سيد أحمد، الحماية القانونية للبيانات الشخصية – دراسة مقارنة في القانون البريطاني والإماراتي، مجلة القضاء والقانون، العدد ٤، ٢٠١٨، ص.٦.

تعقيب: إن نهج المشرع هذا لا يؤثر على مستوى الحماية الممنوحة لهذه البيانات أو على آلية إدارتها. حيث ينبغي أن يشمل الإطار القانوني جميع جوانب وحالات معالجة البيانات الشخصية، وهو ما يتجلى بوضوح في القانون رقم ١٥١ لسنة ٢٠٢٠. لكن لدينا ملاحظات حول فلسفة المشرع ومنهجه في تحديد الأساس القانوني للمعالجة، كما هو موضح في المادة الثانية من القانون حيث نصت المادة الثانية على حظر التعامل في البيانات الشخصية بأي شكل من الأشكال إلا إذا وافق الشخص المعني بالبيانات على ذلك، واشترط المشرع لمعالجة البيانات الشخصية بصفة عامة توافر مجموعة من الشروط نصت عليها المادة الثالثة، وهي:

١. أن تجمع البيانات الشخصية لأغراض مشروعة ومحددة ومعلنة للشخص المعني.
٢. أن تكون صحيحة وسليمة ومؤمنة.
٤. أن تعالج بطريقة مشروعة وملائمة لأغراض التي تم تجميعها من أجلها.
٥. ألا يتم الاحتفاظ بها لمدة أطول من المدة اللازمة للوفاء بالغرض المحدد لها.

وأحال إلى اللائحة التنفيذية في تحديد السياسات والضوابط والمعايير لجمع ومعالجة وتأمين لهذه البيانات.

ونرى أن النصوص التشريعية هذه تجعل من موافقة الشخص المعني بالبيانات سبباً لتقنين معالجة البيانات الشخصية، حيث جاءت المادة السادسة من القانون بالنص على " تعد المعالجة الإلكترونية مشروعة وقانونية في حال توفر أي من الحالات الآتية:

١. موافقة الشخص المعني بالبيانات على إجراء المعالجة من أجل تحقيق غرض محدد أو أكثر.
٢. أن تكون المعالجة لازمة وضرورية تنفيذًا لالتزام تعاقدي أو تصرف قانوني أو لإبرام عقد لصالح الشخص المعني بالبيانات، أو لمباشرة أي من إجراءات المطالبة بالحقوق القانونية له أو الدفاع عنها.
٣. تنفيذ التزام ينظمه القانون أو أمر من جهات التحقيق المختصة أو بناءً على حكم قضائي.
٤. تمكين المتحكم من القيام بالتزاماته أو أي ذي صفة من ممارسة حقوقه المشروعة، ما لم يتعارض ذلك مع الحقوق والحريات الأساسية للشخص المعني بالبيانات."

لم يحدد المشرع أي قيود أو ضوابط للموافقة المطلوبة لمعالجة البيانات الشخصية، سوى أن تكون صريحة كما ورد في المادة الثانية. ومع ذلك، لم يوضح المشرع ما المقصود بالموافقة الصريحة، ولا كيفية تقديمها أو إثبات الحصول عليها بالأخص حال البيانات الحساسة، ويتبادر للذهن تساؤل: هل يجب أن تتوفر موافقة الشخص المعني في جميع الحالات الأخرى للمعالجة المذكورة في المادة السادسة، أم أن موافقة الشخص المعني تعتبر حالة مستقلة ولا تتطلب توافرها في الحالات الأخرى؟

وتلاحظ ايضاً استخدام المشرع عبارة "الأحوال المصرح بها قانوناً" في أكثر من موضع دون توضيح لهذه الحالات، مما يجعل قراءة مواد القانون قد تكون غير واضحة أو غير قابلة للتطبيق. هذه العبارة تفرض قيداً

أو تمنح استثناءً دون توضيح تفاصيله. وقد ساهم في هذا الغموض عدم صدور اللائحة التنفيذية للقانون [١].

ما لم تتوافق المعالجة مع الحالات التي يحددها القانون، يظهر بعض الغموض حول ما تعنيه هذه الحالات. فما هي هذه الحالات وما هو المعيار لتحديدها؟ هل تشير إلى الحالات المستثناة من تطبيق أحكام هذا القانون، كما هو منصوص عليه في المادة الثالثة من مواد الإصدار، أم أنها تختلف عنها؟ هل تتعلق بالحالات المذكورة في المادة السادسة من القانون، التي اعتبرها المشرع حالات قانونية ومشروعة للمعالجة؟

تشير القراءة الأولية للقانون إلى أن عبارة "الأحوال المصرح بها قانوناً" وردت في المواد ١/٤، ٢، ٤/٥، ٥/٥، ١٢، ٣٦، و ٤١، وجميعها تدل على مشروعية معالجة البيانات دون الحاجة للحصول على موافقة الشخص المعني، طالما أن المعالجة تقع ضمن نطاق الأحوال المصرح بها قانوناً. بناءً على ذلك فقد ذهب جانب من الفقه [٢] الى هناك فرضين لتفسير عبارة "الأحوال المصرح بها قانوناً":

(١) دعاء حامد محمد عبد الرحمن، الموافقة ودورها في تقنين التعامل في البيانات الصحية الحساسة وتأثيرها على الأمن المعلوماتي قراءة في قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، بحث مقدم إلى المؤتمر العلمي الدولي الأول لكلية الحقوق جامعة السادات بعنوان الحماية القانونية للإنسان في ضوء التقدم الطبي والتكنولوجي (رؤية مصر ٢٠٣٠ في المجال الصحي) ٣٠ – ٣١ يوليو ٢٠٢٢

(٢) دعاء حامد محمد عبد الرحمن، المرجع السابق.

الفرض الأول: يُفترض أن المقصود هو الأحوال المصرح بها قانونًا، وهي الحالات المستثناة من تطبيق أحكام هذا القانون، كما هو منصوص عليه في المادة الثالثة. ومع ذلك، نرفض هذا الاحتمال لأسباب عدة:

١. لقد قدم المشرع هذه المادة بعبارة "لا تسري أحكام القانون المرافق على ما يأتي:" مما يعني أن البنود التالية مستثناة تمامًا من تطبيق أحكام هذا القانون لأسباب معينة يراها المشرع. وهذا يختلف عن مدلول عبارة "الأحوال المصرح بها قانونًا"، التي تشير إلى أن أحكام هذا القانون ستنطبق عليها ولكن وفق ضوابط خاصة.

٢. كما أن حقوق الشخص المعني بالبيانات، المنصوص عليها في المادة الثانية من القانون، لا يمكن تطبيقها على الحالات المذكورة في المادة الثالثة، للاختلاف الواضح بينهما. فإذا كان من حق الشخص المعني بالبيانات معرفة بياناته الشخصية، والانسحاب من الموافقة المسبقة، وتصحيح وتعديل وحذف بياناته، وتحديد نطاق المعالجة، بالإضافة إلى معرفة حالات الخرق أو الانتهاك، وأخيرًا الاعتراض على المعالجة، فإن هذه الحقوق لا تنطبق على الحالات المستثناة.

٣. إذا كانت البيانات الشخصية تؤدي إلى انتهاك حقوقه وحرياته، فلا يمكن تنفيذ هذه الحقوق أو المطالبة بها إذا كانت المعالجة قد تمت في أي من الحالات المذكورة في المادة الثالثة، وبالأخص في الحالات الثانية والرابعة والخامسة والسادسة منها.

الفرض الثاني: يُعتبر أن الأحوال المصرح بها قانونًا هي تلك المذكورة في المادة السادسة من القانون، وهو ما نذهب معهم إليه بشكل أكبر للأسباب التالية:

١. لقد قدم المشرع هذه المادة بعبارة "تُعد المعالجة الإلكترونية مشروعة وقانونية في حال توافر أي من الحالات الآتية"، مما يدل على أن هذه الحالات تدخل ضمن نطاق تطبيق هذا القانون وتعتبر فيها المعالجة مشروعة.

٢. على الرغم من وجود بعض الغموض واللبس حول طبيعة البنود المذكورة في المادة السادسة، وما إذا كانت هذه البنود تمثل حالات يكفي توافر واحدة منها على الأقل [١]، إلا أننا نرى أن هذه البنود تُعتبر "حالات" مشروعة للمعالجة، كما هو الحال في لائحة الاتحاد الأوروبي.

تعليق: يتلاحظ أن نص المادة السادسة من القانون مترجم من الفقرة الأولى من المادة السادسة من لائحة الاتحاد الأوروبي، التي تشير بوضوح إلى حالات المعالجة المشروعة، مما يجعل الإحالة إليها ضرورية في.

وفيما يتعلق بمعالجة البيانات الشخصية الحساسة، ينص المشرع بوضوح في المادة ١٢ على حظر التعامل مع هذه البيانات إلا بعد الحصول على ترخيص من المركز المختص ، بالإضافة إلى ضرورة الحصول على موافقة كتابية وصريحة من الشخص المعني، باستثناء الحالات التي يصرح بها القانون. يتضح من القراءة الأولية لنص هذه المادة أن المشرع قد اشترط مستوى أعلى من الحماية عند معالجة البيانات الشخصية الحساسة، حيث جعل الأصل هو الحظر إلا في حال توافر الشروط المحددة، وهي:

(١) حيث وضع المشرع لهذه المادة عنوان "شروط المعالجة" ثم قدمها بعبارة " تعد المعالجة الإلكترونية مشروعة وقانونية في حال توفر أي من الحالات التي ذكرها.

١. الحصول على ترخيص لمعالجة البيانات الحساسة من مركز حماية البيانات الشخصية.
٢. الحصول على موافقة كتابية وصريحة من الشخص المعني، باستثناء الحالات المصرح بها قانوناً.

عمد المشرع إلى تعزيز الحماية للبيانات الشخصية الحساسة من خلال فرض شروط معينة لمعالجتها، مما يتعارض مع ما تم النص عليه في المادة الثانية التي كانت تتطلب فقط موافقة الشخص المعني. وهذا يوضح رؤية منهجية للمشرع في تنظيم معالجة البيانات الشخصية الحساسة.

تعقيب: الانتقادات الموجه لقانون حماية البيانات الشخصية:

- اعتمد المُشرِّع في صياغة قانون حماية البيانات الشخصية على فلسفة تقسيم الالتزامات القانونية المرتبطة بحماية البيانات، حيث أحال بعض هذه الالتزامات إلى اللائحة التنفيذية، مبررًا ذلك بأنها قواعد إجرائية تتولى اللائحة تنظيمها.
- كما وُجهت إلى القانون عدة انتقادات، من بينها ارتفاع الرسوم المطلوبة للحصول على البيانات الشخصية، وعدم وجود نصوص واضحة تحدد السياسات والمعايير والضوابط اللازمة لنقل أو تخزين أو مشاركة أو معالجة أو إتاحة البيانات الشخصية عبر الحدود.
- غياب نصوص إجرائية واضحة تنظم عمليات محو وتصحيح وتعديل البيانات الشخصية لدى الحائز أو المُتحكم أو المُعالج.
- وردت الإحالات في ثمانية عشر موضعًا مختلفًا. يُعتبر هذا الأمر من أبرز الإشكاليات التي تؤثر على القانون، إذ إن إسناد تنظيم بعض القواعد بشكل منفرد إلى السلطة التنفيذية، المتمثلة في وزارة الاتصالات،

يجعلها المتحكم الوحيد في كيفية تطبيق القانون وتفسير العديد من قواعده. وهذا يؤدي إلى فقدان قواعد القانون لخاصية التنظيم الذاتي والقدرة على تطبيقها دون الاعتماد على قرارات أو قواعد تنظيمية تصدرها السلطة التنفيذية. يمكن تلخيص هذه القواعد في محاور رئيسية كما يلي:

١. تصنيف التراخيص والتصاريح والاعتمادات وتحديد أنواعها، بالإضافة إلى وضع الشروط الخاصة بمنحها.
٢. تحديد القواعد والشروط والإجراءات والمعايير الفنية المتعلقة بتراخيص وتصاريح اعتماد نشاط جمع البيانات الشخصية.
٣. وضع السياسات والإجراءات والمعايير القياسية لجمع ومعالجة وحفظ وتأمين البيانات داخل وخارج مصر.
٤. تحديد شروط قيد وتسجيل مسؤولي حماية البيانات الشخصية في السجل المخصص بمركز حماية البيانات.
٥. توضيح الالتزامات والمهام لمسؤولي حماية البيانات الشخصية في الجهات المسؤولة عن جمع ومعالجة البيانات.
٦. تحديد حجية الدليل الرقمي المستمد من البيانات الشخصية، والمعايير والشروط الفنية المطلوبة فيه
٧. وضع سياسات ومعايير وضوابط نقل أو مشاركة أو معالجة أو إتاحة البيانات الشخصية عبر الحدود.
٨. توضيح إجراءات وشروط إصدار وتجديد التراخيص والتصاريح، بالإضافة إلى نماذجها المستخدمة.
٩. تحديد رسوم منح التراخيص والتصاريح والاعتمادات للجهات التي تقوم بجمع ومعالجة البيانات.

يتضح أنه من المستحيل البدء الفعلي في تنفيذ القواعد المنصوص عليها في قانون حماية البيانات قبل الانتهاء من إقرار لائحته التنفيذية. كما يتبين تأخر وزارة الاتصالات وتكنولوجيا المعلومات، الجهة المسؤولة عن إصدار هذه اللائحة. ويعود ذلك إلى أن الفلسفة التي اتبعها المشرع عند إصدار قانون حماية البيانات الشخصية أدت إلى تركيز معظم القواعد الأساسية في اللائحة، مما تسبب في تعطيل تطبيق القانون بالكامل بسبب عدم إقرار اللائحة.

ضوابط إجرائية يجب أن تتضمنها في اللائحة التنفيذية

من الضروري صياغة مجموعة من الضوابط الإجرائية في اللائحة التنفيذية لقانون حماية البيانات، بالإضافة إلى الجوانب التي أحال القانون تنظيمها إلى هذه اللائحة. ومن بين هذه الضوابط:

١. ملاءمة إتاحة البيانات الشخصية: يجب أن تتضمن اللائحة مجموعة من الضوابط المتعلقة بكيفية تقديم البيانات الشخصية التي يطلبها المستخدم بشكل ملائم. ينبغي أن يكون للمستخدم الحق في تحديد أو اختيار الطريقة والصيغة التي تناسب احتياجاته.

٢. آلية واضحة للإبلاغ عن الانتهاكات: يجب أن تتضمن اللائحة نصًا صريحًا يحدد آلية إبلاغ المستخدم عن أي انتهاك يتعلق ببياناته الشخصية، بما في ذلك المدة الزمنية التي يجب خلالها إبلاغ المستخدم بحجم الضرر الذي لحق ببياناته.

٣. تنظيم إجراءات تصحيح أو تعديل أو محو البيانات: لا يكفي أن ينص القانون على حق المستخدم في محو أو تعديل بياناته، بل يجب أن تتضمن اللائحة قواعد إجرائية ملزمة تحدد كيفية تقديم الطلب،

والمواعيد المحددة للرد، وحدود مسؤولية المعالج أو المتحكم في حال عدم الامتثال.

النتائج المترتبة على التأخير في إصدار اللائحة التنفيذية: إن تأخير إصدار اللائحة التنفيذية لهذا القانون لم يكن الأول من نوعه. فقد سبق واستغرق إصدار اللوائح التنفيذية للعديد من التشريعات التي أُقرت في السنوات الأخيرة وقتًا طويلاً، قد تصل إلى أكثر من سنتين في بعض الحالات مما يبقى القانون معطلًا كليًا أو جزئيًا مثل، تأخر إصدار اللائحة التنفيذية لقانون تنظيم الإعلام والصحافة (قانون رقم ١٨٠ لسنة ٢٠١٨) ولائحة قانون مكافحة جرائم تقنية المعلومات (قانون رقم ١٧٥ لسنة ٢٠١٨). مما يرتب عدد من الآثار السلبية على التطبيق بشكل عام. وفي سياق مناقشتنا لقانون حماية البيانات الشخصية، يمكن تحديد أثرين مباشرين:

١. **التعطيل الكامل لقانون حماية البيانات الشخصية** خصص المشرع اثني عشر فصلًا لوضع القواعد التنظيمية المتعلقة بالتعريفات الأساسية، وتحديد مسؤوليات الأطراف المختلفة في عملية جمع ومعالجة وتخزين البيانات الشخصية المعالجة إلكترونيًا، ودور الجهات المعنية في تطبيق القانون والفصلان الأخيران، تم تخصيصهما لدور جهات الضبط والتحري، والعقوبات المقررة في حال حدوث أي انتهاكات للقانون وهذا يشير إلى أن قانون حماية البيانات الشخصية يتسم بالطابع التنظيمي، مما يجعله بحاجة إلى لوائح وقرارات تنظيمية لتنفيذه.

إن تطبيق هذه النصوص يعتمد على وضوح القواعد التنظيمية وقابليتها للتنفيذ. على سبيل المثال، مساءلة مقدمي الخدمة عن المخالفات المتعلقة بتنفيذ القانون تتطلب أولاً تحديد الاشتراطات الفنية والاحتياطات

التي يجب على مقدمي الخدمة الالتزام بها، علاوة على ذلك، يُعتبر هذا القانون من القوانين الحديثة بمعنى لا توجد قوانين أو لوائح سابقة يمكن العمل بها بشكل مؤقت.

عدم البدء في تشكيل الهيئات المعنية بتطبيق القانون: تولى معظم القوانين المتعلقة بحماية البيانات الشخصية مسؤولية الإجراءات والضوابط المتعلقة بحماية البيانات إلى هيئات مستقلة، حيث تتابع تنفيذ القواعد المنصوص عليها في القانون.

لقد أنشأ قانون حماية البيانات الشخصية ١٥١ لسنة ٢٠٢٠ م هيئة جديدة تُعرف بـ "جهاز حماية البيانات"، مستلهمًا من اللائحة الأوروبية لحماية البيانات (**GDPR**) التي اعتمد عليها المشرع المصري في صياغة القانون. وقد حدد القانون قواعد تشكيل هذا الجهاز واختصاصاته، ولم يتم إحالة أي من القواعد المنظمة له إلى اللائحة التنفيذية للقانون، مما يعني نظريًا إمكانية البدء في تشكيل الجهاز. ومع ذلك، فإن الواقع العملي يُفرغ هذا التشكيل من محتواه، حيث إن تشكيل الجهاز لا يتطلب إقرار اللائحة التنفيذية، إلا أن ممارسة الجهاز لصلاحياته تبقى معطلة حتى صدور هذه اللائحة ويعتبر تشكيل الجهاز وبدء ممارسة اختصاصاته وصلاحياته مؤشرًا مهمًا على بدء التنفيذ الفعلي لقواعد القانون.

ثالثاً: طبيعة المسؤولية المدنية عن انتهاك خصوصية البيانات الرقمية:

إن تعرض البيانات الشخصية الرقمية إلى الاعتداء عليها من شأنها المساس أو الإضرار بصاحب البيانات الذي تتعرض بياناته إلى الانتهاك، ولذلك كان من اللازم إلقاء الضوء على الحماية المدنية لصاحب الحق لصاحبه، وتمكنه من اللجوء إلى القضاء المدني من أجل إعادة الحال إلى ما كان عليه إذا كان ذلك ممكنا، أو الحصول على تعويض عادل يتناسب

والضرر اللاحق به وفق أحكام وقواعد المسؤولية العقدية أو ناتج عن التزام غير عقدي، والذي تطبق بشأنه قواعد المسؤولية التقصيرية

- **أطراف العلاقة في البيئة الرقمية:** تتداخل عدة أطراف في إتاحة وعرض البيانات على شبكة الإنترنت، انطلاقا من مستخدم الشبكة مرورا بمزود الخدمة الذي يتخذ عدة أشكال، تتمثل في مقدم خدمة الاتصال بشبكة الإنترنت وكذا متعهد الإيواء إضافة إلى مورد المحتوى المعلوماتي وهي أطراف غير مألوفة في نظرية القانون أوجدتها البيئة الرقمية [١]:

(١) مستخدم الشبكة: يعرف مستخدم الشبكة على أنه: "كل شخص يتولّى الإبحار على شبكة الإنترنت مهما كانت طبيعته ودرجة معارفه، وكل من يملك جهاز كمبيوتر شخصي مزود بمودم، واشتراك في الشبكة، يستطيع الحصول على أية معلومة أو كتاب أو صورة فوتوغرافية أو موسيقى معينة أو غيرها بواسطة الشبكة ". مزود الخدمة: (مزود خدمة الإنترنت – متعهد الوصول– متعهد الخدمة) ويعتبر هو الناشر الحقيقي للمعلومة والمنتج لمحتواها، يمكن أن يشغل واقعيا عدة أنشطة فهو منتج للمعلومة، ومزود دخول ومالك المزود (SERVEUR) وموزعا للمعلومة على صفحاته، ويكون في هذه الحالة مسؤولا تقصيريا وعقديا عن المعلومات غير المشروعة، والتي يتم إيواؤها بأنظمة باعتباره تقنيا في الإرسال ". وعليه يعد مزود الخدمة "أي من مقدمي الخدمات الذين يعملون في إطار التواصل على الشبكة ومن أصنافهم: مقدم خدمات النفاذ إلى الشبكة ومقدم خدمات التواصل على الشبكة ومقدم خدمات الاستضافة على الشبكة". ويشمل مقدم التواصل على الشبكة ومقدم خدمات الاستضافة على الشبكة ومقدم خدمات النفاذ إلى الشبكة ومتعهد الإيواء ويطلق " "شركة تجارية أو أحد أشخاص القانون العام، كالجامعات والمؤسسات العامة، والتي تقوم بإيواء صفحات (web) على حساباتها الخاصة وعادة ما يكون ذلك مقابل أجر" ومورد المحتوى المعلوماتي كذلك.

حماية خصوصية البيانات الرقمية بموجب أحكام المسؤولية العقدية:

يرتب العقد الصحيح التزامات على طرفيه، لأن القوة الملزمة للعقد تفيد قيام كل طرف بتنفيذ التزامه، وفي حالة عدم قيام أحد الطرفين بتنفيذ التزامه عينا، وطالبه الدائن أجبر المدين على تنفيذه، وهو أصل الالتزام أما إذا استحال التنفيذ العيني حكم القاضي بالتعويض للدائن إذا طلبه هذا الأخير، وتوفرت شروط الخطأ العقدي والضرر والعلاقة السببية.

- **الخطأ العقدي:** ينشأ الخطأ العقدي بالنسبة لموضوع الدراسة البيانات الرقمية، بقيام الخطأ في حالة عدم احترام مقدم خدمات الإنترنت لبنود العقد المتضمنة أخذ الاحتياطات اللازمة لمنع الدخول إلى البيانات، ولم يقم بتأمين الحراسة اللازمة لمضمون الموزعات المفتوحة للمشتركين في الموقع أو الشبكة ويقع عبء إثبات الخطأ العقدي على عاتق الدائن، فإذا كان محل هذا الالتزام هو تحقيق نتيجة فعلى الدائن إثبات أن هذه النتيجة لم تتحقق، وإذا كان محل الالتزام هو بذل عناية وجب على الدائن في هذه الحالة إثبات عدم قيام المدين ببذل عناية الرجل العادي
- **الضرر:** يتحقق الضرر محل الدراسة بالنسبة إلى تسرب البيانات إذا أخل المدين بالتزامه التعاقدي مما قد يسبب للدائن ضررا ماديا يمس حقوقه المالية أو معنويا، يلتزم هذا الأخير أي الدائن بإثباته.
- **العلاقة السببية بين الخطأ والضرر:** مفاد هذا الركن أن يكون الضرر الذي أصاب الدائن (مالك البيانات) ناتجا عن خطأ المدين مستخدم الشبكة أو مورد المحتوى المعلوماتي...) ويقع عبء إثبات العلاقة السببية بين الخطأ والضرر على عاتق الدائن، ويجوز للمدين نفيه إذا أثبت أن الضرر وقع بسبب أجنبي أو بخطأ الدائن نفسه.

حماية خصوصية البيانات الرقمية بموجب أحكام المسؤولية التقصيرية:

هذا النوع من المسؤولية يقوم في حالة غياب العقد الذي يربط بين مالك البيانات وبين غيره من المستخدمين الغير شرعيين لها، والمسؤولية التقصيرية هي نتاج أو جزاء الفعل الغير مشروع.

وتنص المادة ١٢٤٠ من القانون المدني الفرنسي على أنه: "كل فعل أيا كان يقع من الإنسان ويحدث ضررا للغير يلزم من أوقع هذا الفعل الضار بخطئه بتعويض هذا الضرر، كما تنص المادة ١٦٣ من القانون المدني المصري على أنه: "كل خطأ سبب ضررا للغير، يلزم من ارتكبه بالتعويض"

- **الخطأ:** طبيعة الخطأ في مجال حماية قواعد البيانات: الخطأ في المسؤولية التقصيرية هو: "إخلال بالتزام قانوني الذي يعتبر الإخلال به خطأ في المسؤولية التقصيرية فهو دائما التزام ببذل عناية، وهو أن يراعي الشخص في سلوكه اليقظة والتبصر حتى لا يضر بالغير، ويشترط لقيامه توفر عنصرين عنصر مادي، ويتمثل في التعدي البين، وعنصر معنوي يتمثل في النية، إذ لا يمكن نسبة الخطأ إلى شخص فاقد للتمييز. ويقوم الخطأ محل الدراسة، بالتعدي على أحد الحقوق الشخصية، كالدخول الغير مرخص على البيانات، أو القيام باستنساخها أو استعمالها في غير الحالات الاستثنائية المرخصة لذلك، أو القيام بإعادة نشرها بدون ترخيص.
- **الضرر:** يشمل الضرر "تفويت كسب مادي مشروع للمضرور أو المساس بسمعته، وهذا الضرر يجب إثباته، ويشترط في هذا الضرر أن يكون محققا، إذ أنه لا تعويض عن الأضرار المحتملة حتى يتحقق الضرر فعلا.

- **العلاقة السببية:** تعتبر العلاقة السببية هي الرابطة بين الخطأ التقصيري، والضرر الذي أصاب المضرور من تسرب والاستخدام غير المشروع للبيانات إذ يستلزم على هذا الأخير إثبات هذه العلاقة.

علاقة السببية في مجال البيانات الرقمية: إثبات قيام العلاقة السببية في مجال البيانات الرقمية، أو في المجال الإلكتروني بصفة عامة مسألة معقدة، نظراً لتعقد الظاهرة الالكترونية، وتشعبها، فقد يعود سبب الضرر الذي يصيب مالك البيانات إلى الأجهزة المستعملة، أو مزود خدمة الإنترنت أو مقدمها، وهو ما يصعب معه تحديد السبب الرئيسي في الضرر.

وخلاصة القول في ظل القانون المصري رقم ١٥١ لسنة ٢٠٢٠ الحاكم بحماية البيانات وخصوصية البيانات الرقمية إذا تحققت أركان المسؤولية (عقدية / تقصيرية) نتيجة فعل التعدي من خطأ وضرر وعلاقة سببية وجبت المسؤولية والتعويض.

نتائج البحث:

١. على الرغم من وجود دول تمتلك تشريعات تهدف إلى حماية خصوصية مواطنيها من سرقة البيانات الشخصية أو التجسس أو استغلالها لأغراض تجارية وإعلانية، إلا أن هذه التشريعات تعاني من نقص في الوضوح وتحتوي على العديد من الثغرات القانونية. يعود ذلك إلى اعتمادها على معايير قديمة، مما يجعلها غير قادرة على التعامل مع جميع الحالات التي تهدد خصوصية البيانات الرقمية.
٢. أصبح تنظيم التعامل مع البيانات الشخصية ضرورة لا مفر منها في ظل التطور السريع لقوة البيانات وتأثيرها على اتخاذ القرارات وإدارة الأعمال.

٣. لا يمكن فصل تنظيم التعامل مع البيانات الشخصية عن أهداف التنمية المستدامة للدولة.
٤. يُعتبر أمن البيانات والمعلومات جزءًا لا يتجزأ من استقرار المجتمع، وهو مرتبط ارتباطًا وثيقًا بالأبعاد الاجتماعية والاقتصادية والبيئية التي تستند إليها استراتيجية مصر للتنمية المستدامة.
٥. تأثر المشرع المصري بلائحة الاتحاد الأوروبي عند وضع قانون حماية البيانات الشخصية، واستمد منها العديد من الأحكام.
٦. قام المشرع بتعزيز مستوى الحماية للبيانات الشخصية الحساسة من خلال فرض مجموعة من الشروط لمعالجتها، مما يتعارض مع ما ورد في المادة الثانية التي كانت تتطلب فقط موافقة الشخص المعني بالبيانات. وهذا يعكس بوضوح رؤية المشرع ومنهجه في تنظيم معالجة البيانات الشخصية الحساسة.
٧. إن القراءة المتأنية لنص المادة السادسة من القانون ١٥١ لسنة ٢٠٢٠ تكشف عن وجود خلل واضح في صياغة المادة، مما يؤدي إلى إمكانية حدوث نزاع حول تطبيقها وتفسيرها. يعود السبب في ذلك إلى أن عنوان المادة "ثالثاً: شروط المعالجة" يشير بوضوح إلى أن كلمة "شروط" تعني ضرورة توافر جميع الشروط لتحقيق الأثر القانوني للفعل. وبالتالي، يجب توافر الشروط الأربعة، بما في ذلك شرط الموافقة، حتى تكون معالجة البيانات مشروعة وقانونية.

ومع ذلك، نجد أن المشرع ابتدأ المادة بعبارة "تعد المعالجة الإلكترونية مشروعة وقانونية في حال توفر أي من الحالات الآتية:" ثم ذكر الحالات الأربعة. ومن الواضح أن عبارة "أي من الحالات الآتية" تعني أن هناك خياراً بين هذه الحالات، بما في ذلك حالة موافقة الشخص المعني

بالبيانات، مما يعني أنه يكفي توافر حالة واحدة فقط لتكون المعالجة قانونية ومشروعة. إذن، يبقى السؤال: ما هو التفسير الصحيح لهذه المادة؟

٨. يُلاحظ أن قانون حماية البيانات الشخصية يعاني من عدم وضوح أو دقة بعض المصطلحات، مما قد يثير لبسًا لدى المختصين عند تطبيقه.

٩. اعتبر المشرع المصري موافقة الشخص المعني بالبيانات شرطًا أساسيًا لتقنين التعامل مع البيانات الشخصية بشكل عام، والبيانات الحساسة بشكل خاص.

١٠. اشترط المشرع الحصول على موافقة كتابية وصريحة لمعالجة البيانات الحساسة، بالإضافة إلى تصريح من مركز حماية البيانات الشخصية، مما يعكس توجه المشرع نحو تشديد إجراءات معالجة هذا النوع من البيانات.

التوصيات:

١. يجب على الجهات المعنية في الدولة العمل على نشر ثقافة حماية البيانات وزيادة الوعي لدى الجمهور والمؤسسات بأهمية الالتزام بإجراءات الحماية المنصوص عليها قانونياً.

٢. من الضروري تحديد ضوابط موافقة الشخص المعني بالبيانات بشكل واضح في المادة الأولى من القانون، وتوضيح المقصود بالموافقة الصريحة.

٣. ينبغي إعادة صياغة نص المادة السادسة من القانون وتوضيح نية المشرع من المادة السادسة من القانون ١٥١ لسنة ٢٠٢٠، من خلال اللائحة التنفيذية للقانون أو بتعديل المشرع لها. ومن الواضح أن هذه المادة ليست سوى ترجمة وتعريب لنص المادة ٦.١ من لائحة الاتحاد

الأوروبي، التي تحدد حالات مشروعية معالجة البيانات الشخصية. حيث ذكرت تلك اللائحة ست حالات، يكفي تحقق واحدة منها لتكون المعالجة مشروعة.

٤. يجب توضيح المقصود بعبارة "في الأحوال المصرح بها قانوناً" التي وردت في عدة مواضع من القانون.

٥. تتناول هذه الورقة مجموعة من الإشكاليات المتعلقة بتأخر إصدار اللائحة التنفيذية لقانون حماية البيانات الشخصية، والظروف المحيطة بعملية الإقرار. ويعتمد حل هذه الإشكاليات على أمرين رئيسيين:

الأول: ضرورة تحديد إطار زمني واضح ومعلن لإنهاء عملية إقرار اللائحة التنفيذية لقانون حماية البيانات الشخصية. كما يجب تطبيق قواعد ومعايير الشفافية خلال مراحل الإقرار، مع توضيح أي معوقات قد تطرأ، والإعلان عن أي تغييرات في الجدول الزمني بشكل علني.

الثاني: أهمية تعزيز الحوار المجتمعي من خلال قواعد جادة تشمل جميع الفئات المختلفة في عملية وضع اللائحة. وذلك لتفادي الأخطاء التي وقعت أثناء صياغة قانون حماية البيانات.

٦. حدد مركز حماية البيانات الشخصية مقابل بما يتجاوز عشرين ألف جنيه، وهو مبلغ مرتفع قد يعيق الشخص المعني عن ممارسة حقوقه التي يكفلها له القانون والدستور فيما يتعلق بحماية بياناته الشخصية. لذا، ينبغي على المركز عند تحديد أسعار الخدمات أن يأخذ في الاعتبار وضع رسوم تتناسب مع طبيعة البيانات الشخصية التي تحتاج إلى الحماية

٧. غالبًا قد لا تعتمد الأجهزة الأمنية على إذن قضائي يسمح لها بممارسة المراقبة، مما يؤدي إلى انتهاك حق المواطن في معرفة ما إذا كان تحت

المراقبة أم لا، ويتجاوز حقه في رفض ذلك. لذلك، ينبغي أن تستند عمليات المراقبة إلى أمر قضائي، وأن تتم تحت إشراف هيئة مستقلة عن الأجهزة الأمنية. يجب أن تضمن هذه الهيئة عدم وصول البيانات الشخصية للأفراد إلى الجهات غير الحكومية، كما تتولى الإشراف على تطبيق القوانين التي تحمي البيانات الشخصية.

٨. إن من أهم أحد العوامل الرئيسية التي تساهم في حماية خصوصية البيانات الرقمية للأفراد ليس فقط وضع القوانين، بل يتطلب أيضاً التأكد من تنفيذها ومرونتها للتعديل استجابةً لأي انتهاكات قد تؤثر على خصوصية البيانات الرقمية.

خاتمة:

في ختام هذا البحث، نود أن نؤكد على أهمية موضوع الحماية القانونية للخصوصية الرقمية في العصر الرقمي الحالي، حيث أصبح ضمان الحفاظ على خصوصية المعلومات الشخصية والبيانات الحساسة أثناء استخدامها ومعالجتها في البيئة الرقمية أمرًا بالغ الأهمية. سعى البحث لإبرازها من خلال بيان أهمية حماية حقوق الأفراد في الحفاظ على خصوصيتهم والسيطرة على بياناتهم الشخصية، والتحكم في كيفية جمع واستخدام هذه البيانات من قبل المؤسسات والشركات.

سعى البحث نحو الإسهام في ابراز أهمية صياغة التشريعات واللوائح المتعلقة بحماية البيانات الشخصية هو أحد الأهداف الأساسية لهذا البحث، حيث يساعد ذلك في تطوير نصوص قوانين فعالة توفر إطارًا قانونيًا للشركات والمؤسسات للامتثال لمتطلبات الخصوصية. بالإضافة إلى التصدي للتهديدات السيبرانية من خلال فهمها وتطوير استراتيجيات للحفاظ على سرية البيانات.

كما تناول البحث أهمية التوجيه بسن تشريعات جديدة مثل اللائحة التنفيذية لقانون حماية خصوصية البيانات ١٥١ لسنة ٢٠٢٠ م.

أو تعديل التشريع القائم للتعامل مع التحديات الناشئة في مجال حماية البيانات، مما يؤثر في بناء الثقة في البيئة الرقمية بين المستخدمين والمؤسسات، ويعزز التفاعل الإلكتروني ويحفز على استخدام التكنولوجيا بثقة.

ساهم البحث أيضًا في ابراز أهمية تحقيق توازن بين استفادة المجتمع من التقنيات والبيانات وبين حماية حقوق الأفراد وخصوصياتهم، مما يعمل على تطوير بيئة رقمية آمنة ومستدامة في ظل حماية تشريعية فعالة.

حاول البحث في ايجاد كيفية لتوفير الحماية القانونية لخصوصية المعلومات الرقمية لمستخدمي شبكات الإنترنت، وإيجاد حلول للمشكلات القانونية الناتجة عن استخدام مواقع الشبكات الاجتماعية، وفقًا لقانون حماية خصوصية البيانات ١٥١ لسنة ٢٠٢٠ م.

ختامًا، نأمل أن يسهم هذا البحث في تعزيز الفهم العميق للتحديات والفرص المتعلقة بحماية البيانات الشخصية في البيئة الرقمية، ويساعد في تطوير تشريعات فعالة تضمن حماية خصوصية البيانات الرقمية وتعزز الثقة في المعاملات الالكترونية.

قائمة المراجع:

المراجع العربية

١. الشيخ الحسين محمد يحي وسيد محمد سيد أحمد، الحماية القانونية للبيانات الشخصية – دراسة مقارنة في القانون البريطاني والإماراتي، مجلة القضاء والقانون، العدد ٤٠، ٢٠١٨.

٢. بارق منتظر عبد الوهاب، جريمة انتهاك الخصوصية عبر الوسائل الالكترونية في التشريع الأردني دراسة مقارنة، رسالة ماجستير مقدمة لكلية الحقوق جامعة الشرق الاوسط، ٢٠١٧.

٣. حسام الدين الأهواني. الحق في احترام الحياة الخاصة دراسة مقارنة، دار النهضة العربية، القاهرة، ١٩٧٨.

٤. حاتم أحمد محمد بطيخ، دراسة تحليلية مقارنة لنصوص قانون مكافحة جرائم تقنية المعلومات الواردة في قانون مكافحة جرائم تقنية المعلومات المصري، رقم ١٧٥ لسنة ٢٠١٨، بنك المعرفة المصري.

٥. دعاء حامد محمد عبد الرحمن، الموافقة ودورها في تقنين التعامل في البيانات الصحية الحساسة وتأثيرها على الأمن المعلوماتي قراءة في قانون حماية البيانات الشخصية رقم ١٥١ لسنة ٢٠٢٠، بحث مقدم إلى المؤتمر العلمي الدولي الأول لكلية الحقوق جامعة السادات بعنوان الحماية القانونية للإنسان في ضوء التقدم الطبي والتكنولوجي (رؤية مصر ٢٠٣٠ في المجال الصحي) ٣٠-٣١ يوليو ٢٠٢٢.

٦. عبد المجيد غمجيه، الحماية القضائية للمعطيات الشخصية، المعهد العالي للقضاء.

٧. طارق جمعة السيد راشد، الحماية القانونية لخصوصية البيانات الشخصية في العصر الرقمي، مجلة القانون والاقتصاد، العدد ٩٢، ٢٠١٩.
٨. طارق جمعة السيد راشد، الحماية القانونية للحق في خصوصية البيانات الجينية – دراسة تحليلية مقارنة، المجلة القانونية، مجلد ٨، العدد ١٢، ٢٠٢٠.
٩. طارق عثمان، الحماية الجنائية للحياة الخاصة عبر الإنترنت، رسالة ماجستير سنة ٢٠٠٦-٢٠٠٧.
١٠. فوزية شريف، التطور التاريخي للحق في الخصوصية بين النصوص الدينية والأحكام الوصفية دراسة تحليلية، بحث منشور ومشارك في كتاب أعمال المؤتمر الدولي المحكم حول الخصوصية في مجتمع المعلوماتية، ٢٠١٩.
١١. سامح عبد الواحد التهامي، "ضوابط معالجة البيانات الشخصية: دراسة مقارنة بين القانون الفرنسي والقانون الكويتي"، مجلة القانون الكويتية العالمية، العدد ٩، السنة ٣، مارس ٢٠١٥.
١٢. شلوح ميرة، بشيرى كهينة، "المسؤولية المدنية عن انتهاك حق الخصوصية في المجال الرقمي"، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة عبد الرحمن ميرة – بجاية، ٢٠١٩-٢٠٢٠.
١٣. محمد أحمد المعداوي حماية الخصوصية المعلوماتية للمستخدم عبر شبكات التواصل الاجتماعي دراسة مقارنة بحث منشور في مجلة كلية الشريعة والقانون بطنطا، ع٣٣، ج ٤، مصر، ٢٠١٨.

١٤. منى الأشقر جبور ومحمود جبور "البيانات الشخصية والقوانين العربية الأمنية وحقوق أفراده"، المركز العربي للبحوث القانونية والقضائية، الطبعة الأولى، بيروت، لبنان، عام ٢٠١٨.

١٥. منى تركي الموسوي والمدرس جان سيريال فضل الله، الخصوصية المعلوماتية وأهميتها و مخاطر التقنيات الحديثة عليها، مركز بحوث السوق وحماية المستهلك، بحث منشور بمجلة كلية بغداد للعلوم الاقتصادية العدد٢٩ الخاص بمؤتمر الكلية، سنة٢٠١٣.

١٦. هشام فريد رستم قانون العقوبات ومخاطر تقنية المعلومات، مكتبة الآلات الحديثة، ١٩٩٢.

١٧. يونس عرب موسوعة القانون وتقنية المعلومات، قانون الكومبيوتر، منشورات اتحاد المعارف العربية، طبعة أولى، ٢٠٠١.

المراجع الأجنبية:

المراجع الإنجليزية:

1. Article 4/13 states: ‘genetic data’ means personal data relating to the inherited or acquired genetic characteristics of a natural person which give unique information about the physiology or the health of that natural person and which result, in particular, from an analysis of a biological sample from the natural person in question.
2. Children’s Online Privacy Protection Act of 1998.
3. Convention for the Protection of Human Rights and Fundamental Freedoms.
4. Data Protection Laws of the World, March 2013.
5. EU’s General Data Protection Regulation (GDPR) 679 / 2016.
6. FTC Staff Issues Privacy Report, Offers Framework for Consumers. Businesses and Policymakers.

7. Gramm-Leach-Bliley Act – Bureau of Consumer Protection.
8. Personal Data Protection Act 2012 – REPUBLIC OF SINGAPORE.

المراجع الفرنسية

1. Cynthia chassigneux, L'encadrement juridique du traitement des données personnelles sur les sites de commerce en ligne, Thèse, Université Panthéon-Assas, Paris II, 2003, nº 278.

الأحكام والقوانين:

١. القانون المصري لحماية خصوصية البيانات ١٥١ لسنة ٢٠٢٠ م الصادر بتاريخ ١٣ يوليو ٢٠٢٠. الجريدة الرسمية ٢٨ مكرر (هـ).
٢. الدستور المصري لعام ٢٠١٤.
٣. العهد الدولي الخاص بالحقوق المدنية والسياسية– المادة ١٧.
٤. القانون رقم ١٩٤ لسنة ٢٠٢٠،
٥. اتفاقية ١٠٨ اتفاقية حماية الأشخاص تجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي التي تمت المصادقة عليها ١٩٨٠.

روابط المواقع الإلكترونية:

1. https://www.cst.gov.sa/ar/Digitalknowledge/Pages/personaldata.aspx
2. https://journals.ekb.eg/article_30623_1ab2f80af612aa4568dbf6239b5
3. http://www.ism.ma/basic/web/pdf/docetude/autre/autre2.pdf
4. : https://jilre.com
5. https://jdl.journals.ekb.eg/article_191190_a30e591b0e0d147fc7926c2b98b33217.pdf
6. http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=EN
7. https://www.iasj.net/iasj/download/51b569f8c8bd04b7