دور المنظمات الدولية في تعزيز الحق في الخصوصية: حماية البيانات الشخصية في البيئة الرقمية

نشوان تكليف جيثوم

DOI:10.15849/ZUJJLS.260730.11

كلية الحقوق، جامعة النهرين، العراق.
***للمراسلة:** nashwanalfarhood@law.nahrainuniv.edu.iq

تاريخ استلام البحث:13/09/2025
تاريخ قبول البحث: 01/11/2025

الملخص

نعيش اليوم في عالم تجتاحه ثورة تكنولوجية بجوانبها المختلفة، ولعل الجانب الأبرز فيها هو الإعلام والاتصالات. حيث أصبح التعاطي مع مختلف جوانب الحياة، بما فيها التعاملات الرسمية والتجارية محكومة ببيئة رقمية تحتوي على حيز من البيانات الشخصية عن الأفراد الطبيعيين. ومن الثابت أن حياة الإنسان ورفاهيته قد تأثرت إيجابياً بشكل لافت نتيجة لتلك الابتكارات، ما انعكس على دعم مسيرة التقدم في الحياة بجوانبها المختلفة. غير أن الجانب الآخر لتلك التكنولوجيا الرقمية، قد حمل في طياته انتهاكاً لحقوق الإنسان الأساسية، وعلى وجه التحديد حقه في خصوصية حياته، وذلك بجعل بياناته الشخصية الخاصة عرضة للكشف بطرق ووسائل تحمل من التلاعب والغش والاحتيال ما يشكل تعدياً على أسرار وتفاصيل شخصية، ما كان ليقبل بها الشخص الطبيعي لو علم أن مستودع بياناته التي أدلى بها لجهة معينة، سوف يقع بين أيادي سواها من الغير، بحيث لا يعلم على وجه التحديد من هي تلك الجهات، وكيف سيتم استغلاله جراء ذلك. ونتيجة لذلك، تصدت العديد من المنظمات الدولية لتلك الممارسات، من خلال الاتفاقيات وإعلان المبادئ والإرشادات التوجيهية، التي تطلب من الدول تعزيز كفالة حقوق الإنسان، من خلال تشريع أو تعديل التشريعات النافذة، بالشكل الذي يواجه به التطور المستمر للتكنولوجيا الرقمية، ما يقلل الفجوة الحاصلة في قوانينها، بالحيثية التي تكفل حق الإنسان في حماية سرية وخصوصية بياناته الشخصية من الكشف والاستغلال غير القانوني لها.

الكلمات الدالة: بيئة رقمية، خصوصية، بيانات شخصية، منظمات، تشريعات، حقوق.

The Role of International Organizations in Enforcing Data Privacy: Personal Data Protection in the Digital Age

Nashwan Takleef Jaythoom

Faculty of Law, Al-Nahrain University, Republic of Iraq.
*** Crossponding author: nashwanalfarhood@law.nahrainuniv.edu.iq**

Recived:13/09/2025
Accepted:01/11/2025

Abstract

Nowadays, we live in a world swept by a technological revolution in its various aspects, perhaps the most prominent of which is media and communications. Interactions in various aspects of life, including official and commercial transactions, are now governed by a digital environment containing a wealth of personal data about individuals. It is well established that human life and well-being have been significantly positively impacted by these innovations, which has supported the progress of life in all its aspects. However, the other side of this digital technology has entailed a violation of basic human rights, specifically the right to privacy. This exposes personal data to disclosure in ways and means that involve manipulation, fraud, and deception. This constitutes an infringement on personal secrets and details, which a natural person would not accept if they knew that the data they provided to a specific entity would fall into the hands of others, without knowing precisely who those entities are and how they will be exploited as a result. As a result, many international organizations have addressed these practices through agreements, declarations of principles, and guidelines. These agreements require states to strengthen human rights protection by enacting or amending existing legislation to address the ongoing development of digital technology. This will narrow the gap in their laws, ensuring that the right to confidentiality and privacy of personal data is protected from unlawful disclosure and exploitation.

Keywords:Digital age, privacy, personal data, organizations, legislation, rights.

المقدمة

يحتل الإنسان وحقوقه الأساسية المكانة والمحور الأساس في ميثاق الأمم المتحدة، وما تمخض عنه من إعلانات ومبادئ واتفاقيات، موضوعها الأساس حقوق الإنسان الأساسية أو طائفة منها. ويأتي حق الإنسان في العيش بحرية وكرامة في مقدمة تلك الحقوق، ويعد حق الإنسان تجاه الكافة في احترام خصوصيته وتحسينها، ترجمة وتفعيل لتلك الحقوق.

ويندرج تحت إطار الخصوصية، حق الإنسان في صون حرمته في المسكن والمراسلات وسرية بياناته الشخصية على اتساع نطاقها. ونتيجة للتطور الهائل في تكنولوجيا المعلومات، والدهشة التي أصابت سكان العالم جراء هذا التحول المتسارع في أنماط الحياة واجتياح التكنولوجيا لمختلف تفاصيلها، نطلق أحيانا تسمية عصر التكنولوجيا على الحقبة الحالية التي نعيش أيامها، بفعل عصف التأثيرات التي نفذت إلى مفاصل الحياة الرئيسية، والتي تحمل طابع أو صبغة الثورة المعلوماتية.

كما لا ينكر التحسن والتقدم الذي نعيشه في عالم اليوم بفضل التطورات والنقلات التي أحدثتها التكنولوجيا، والتي أسهمت في نقل الإنسان من واقع إلى آخر يختلف ويتميز بدرجة كبيرة رقيا وتقدما عما كان عليه حال حياته في السابق، وضمن عقود معدودة من الزمن. ولكن هناك تأثيرات سلبية لهذا العالم الرقمي الذي نحيا في خضمه، ومن أكثر من جانب.

فقد أضحت البيئة الرقمية تمثل صندوق بيانات ومعلومات وأسرار الفرد، الذي قد يضمن أحيانا أن تفاصيل حياته في مأمن، لا يمكن لمن سواه الاطلاع عليها. وهذا أمر مناف للواقع، حيث بدت الكثير من خفايا التأثيرات السلبية للبيئة الرقمية تتكشف، ومنها انتهاك الحق في الخصوصية، بما فيها الخصوصية الرقمية، ما يشكل خرقا لأحكام القانون الدولي ودساتير الدول وقوانينها، على اختلافها. ما يستدعي البحث عن معالجات قانونية للحد من تلك الانتهاكات والتصدي لها، وعلى مستويات متنوعة.

إشكالية البحث

مما لا شك فيه أن هناك العديد من المنظمات الدولية التي تهتم وترعى حقوق الإنسان، وتبذل الجهود من أجل رفاهه وصون كرامته الشخصية. فهل تصدت المنظمات الدولية بما يكفي لحالة التعدي على بيانات الفرد الشخصية في البيئة الرقمية. وما هو الدور الذي لعبته أو تستطيع أن تمارسه تلك المنظمات في هذا الخصوص، وما هي البيانات الشخصية التي تتجسد فيها خصوصية الفرد في البيئة الرقمية، وكيف تكون عليها الحالات التي يتم من خلالها التعرض بسوء لتلك البيانات.

أهمية البحث

يتنقل الفرد في البيئة الرقمية من أبوابها المتسعة النطاق، تاركا جملة من البيانات الشخصية، تارة بإرادته الحرة، وأخرى استجابة لمتطلبات الحياة المتنوعة، من الحصول على الخدمات لدى جهات حكومية وما سواها، الأمر الذي يجعل من حياته الخاصة وتفاصيلها في متناول جهات لا يعلمها، وبحالة انتقال ومداورة، ما يسبب له

أضرارا ومخاطر على أكثر من جانب، ليس أقلها التأثيرات النفسية وكشف دقائق الحياة الخاصة، إلى ما دونه من تأثيرات اجتماعية أو مخاطر اقتصادية وقانونية.

أهداف البحث

يسعى البحث إلى التأكيد على ضرورة ترصين حماية البيانات الشخصية للأفراد، وعدم العبث بها واستغلالها خلافا لإرادته. ما يتطلب بذل الجهود ومن خلال المنظمات الدولية لإدراك ذلك، سواء من خلال إعلان المبادئ والتوصيات أو إبرام المعاهدات ذات الصلة أو تعزيز النافذ منها ببروتوكولات، كما لها اليد العليا في بعض الأحيان في التنسيق بين الدول للوصول إلى مشتركات تتطلب التعاون للتصدي لتلك الممارسات على الصعيدين الداخلي والدولي، سيما أن خرق البيانات الشخصية في حالات عدة يتم عبر شركات عالمية ذات نفوذ وصلات عابرة للحدود.

منهجية البحث

اعتمد البحث المنهج الوصفي في تناوله لأحكام وبنود المعاهدات والإعلانات والمواثيق الدولية، بانيا التحليل والتسبيب والاستنباط من خلال الاستعانة بالمنهج الاستقرائي والوصفي، للوصول إلى قيمة الضمانات القانونية المتوفرة لمواجهة التحديات التي تحيط بخصوصية الفرد، مسلطا الضوء على الثغرات التي يجب العمل على مواجهتها بغية الحد من تلك الانتهاكات.

هيكلية البحث

قسم البحث إلى مطلبين، تناول الأول تبيان ماهية البيانات والمعلومات التي تمثل خصوصية الفرد، والتي تكون متوافرة في البيئة الرقمية، والكيفية التي يتم استغلالها والكشف عنها خارج إطار الغرض الذي حفظت لأجله. في حين يتناول المطلب الثاني الحماية القانونية الدولية لحق الفرد في خصوصية بياناته الرقمية، ومدى فاعليتها في ظل التطور الحاصل في مضمار البيئة الرقمية.

المطلب الأول

البيانات الرقمية الشخصية وطرق التعدي عليها

أضحت البيئة الافتراضية الرقمية هي الحاضن لبياناتنا الخاصة ومستودع أسرارنا. لذلك سنخوض في ثلاثة فروع، من خلال الفرع الأول نبين مضمون تلك البيانات، ويأتي الفرع الثاني على توضيح المقصود بالبيئة الرقمية، ليتناول الفرع الثالث الحالات التي تنتهك من خلالها بياناتنا الرقمية، وأكثر الجهات التي توغل بتلك الممارسات.

الفرع الأول: تعريف البيانات الشخصية

تعد البيانات الشخصية وحرمتها حقا لأصحابها، فهي أحد أوجه الحق في الخصوصية، الذي يعد بدوره من أهم الحقوق الأساسية للإنسان. والحق في الخصوصية يعني "التسليم بحق الأفراد في التمتع بفسحة للتنمية الذاتية، تقوم على مبدأ التفاعل والحرية، أو حقهم في المجال الخاص، يتسع لهم فيه التفاعل أو عدم التفاعل مع الآخرين دون الخضوع إلى تدخل الدولة ولا إلى تدخل تطفلي زائد يمارسه أفراد آخرون بلا دعوة"([1]).

إذن يتضمن الحق في الخصوصية السرية والتخفي والعزلة، فهو حق للإنسان في حماية حياته الخاصة وشؤونه العائلية من التدخل، سواء أخذ ذلك التدخل الطابع المادي، أو طريق النشر للبيانات([2]). فهو قدرة الشخص على السيطرة والتحكم من حيث الكم أو الزمن في الكشف عن التفاصيل الخاصة بحياته للآخرين([3]).

إلا أن التطور في تقنيات المعلومات والاتصالات، أخرج الخصوصية من مفهومها المادي، كمراقبة الأشخاص أو الاطلاع ماديا على بيوتهم وأسرارهم، حيث أصبح كشف كل ذلك ممكنا عبر التقنيات الحديثة، التي جسدت الوجه العصري للخصوصية، والمتعلق بكل ما له صلة بالبيانات الرقمية، وهو ما بات يعرف بحق الإنسان في خصوصيته في البيئة الرقمية، أي الحفاظ على بياناته ومعلوماته التي دونها إلكترونيا، وعدم استخدامها بشكل لا يتفق وإرادة صاحب البيانات([4]).

أما المقصود بكلمة "بيانات" فهو كلمات أو صور أو أرقام أو رموز أو حروف ذات صلة بموضوع معين، ولا يشترط فيها التنسيق أو الترتيب. كأرقام الاستبيانات أو أسماء العمال في منشأة معينة أو صور أو أنشطة وحرف يدوية. وبالتالي قد تكون حقائق موضوعية لا يحكمها الترابط أو التنظيم، حيث يتم الحصول عليها من خلال البحث والتدوين أو بواسطة الملاحظة. وتستخدم تلك المعطيات غير المنتظمة فيما بعد بحسب الغاية المتوخاة من عملية الرصد، فقد يهدف من خلال جمعها إلى الوصول لنتائج أو تحليلات، يخطط من خلالها إلى موضوع ما.

في حين أن البيانات الشخصية هي التفاصيل التي تكون على شكل كلمات أو أرقام أو أية دلالات، وبصرف النظر عن المصدر الذي استقت منه أو الشكل الذي تم العرض به، يمكن من خلالها الاستدلال على شخص طبيعي والتعرف عليه بصورة مباشرة أو غير مباشرة. ومثالها الأسماء أو المهنة أو أرقام تحمل إشارات ذات معنى استدلالي، كأرقام حسابات بنكية أو وسائل التواصل أو لوحات مركبة، أو عناوين السكن أو العمل، أو البصمة البيومترية، أو ممتلكات شخصية، أو خصائص جسدية، أو بيانات الموقع[5].

([1]) الوثيقة رقم A/HRC/39/29 ملحق تقرير مفوض الأمم المتحدة السامي لحقوق الإنسان حول الحق في الخصوصية في العصر الرقمي، 3 آب 2018، ص 3.

([2]) ياسمين بنت نبي بالعسل ، مقدر نبيل، الحق في الخصوصية الرقمية، مجلة المستقبل للدراسات القانونية والسياسية، المجلد 5، العدد 1، 2021، ص6.

([3]) رؤى سعد القرني، الحماية القانونية للحق في الخصوصية المعلوماتية: دراسة مقارنة، مجلة كلية الدراسات الإسلامية والعربية للبنات، الجزء الأول، العدد 6، 2021، ص1036.

([4]) فطيمة نساخ، حماية الحق في الخصوصية في ظل البيئة الرقمية، المجلة الأكاديمية للبحث القانوني، المجلد 13، العدد 1، 2022، ص 419.

([5]) المادة (4) من قانون حماية البيانات العامة للاتحاد الأوروبي (GDPR) 679/2016، اعتمدت من قبل البرلمان والمجلس الأوروبي بتاريخ 27 نيسان 2016.

إذن هناك عدة عناصر تعد الأساس الذي يبنى عليه تصنيف البيانات على أنها تحمل طابع "الشخصية". وهي:

أولا: عنصر المعلومة: يتسم هذا العنصر بالعمومية والشمولية، وتكمن شموليته من جهة كونه غير مقيد بصيغة معينة، حيث تكون المعلومة ذاتية، كالتقييم الشخصي للأهل أو الأصدقاء، وموضوعية مثل العمر. فالبيانات على اختلاف صورها، رقمية أو ما سواها، يمكن أن تأخذ طابع البيانات الشخصية، متى ما دلت بشكل أو بآخر على توصيف أو حالة نفسية متكونة لدى الفرد تجاه أفراد أو مجتمع أو تعبير عن شعور يصف الحالة التي يكون عليها.

ثانياً: دلالة المعلومة: العامل الفاصل في المعلومة سواء كانت صحيحة أم لا، هو نسبتها إلى شخص معين، حينها يمكن وصف البيانات على أنها شخصية، وإن كانت في الواقع تتعلق بشخص آخر. أما كون البيانات تحمل طابع العشوائية، ولا يمكن نسبتها إلى فرد معلوم، فهنا تنزع صفة الشخصية عن تلك البيانات.

ثالثاً: التحديد وقابلية التحديد: المقصود بالتحديد هنا هو التمييز، أي تمييز الفرد عن غيره. سواء كان ذلك التمييز حاسما مباشرا قاطعا، أو بصورة غير مباشرة، من خلال القدرة على التعرف على الفرد من خلال تلك البيانات بعد التجميع والمعالجة مستخدما معلومات أخرى متوافرة أو ممكنة الوصول. والمعرفات كثيرة، منها المعرف الإلكتروني أو البيانات البيومترية كبصمة العين أو الأصابع، وهناك معرفات أكثر تعقيدا من ذلك مثل عنوان بروتوكول الإنترنت (IP). كذلك توجد عوامل تعريفية أخرى تتعلق بهوية الفرد الجينية أو العقلية أو الفسيولوجية. وتشكل تلك العوامل خصائص تسهم في الكشف عن هوية الفرد كونها مرتبطة به[1].

رابعا: الشخص الطبيعي: ليس بالضرورة أن تنسب البيانات المتوافرة في البيئة الرقمية إلى شخص طبيعي، فهناك الأشخاص الاعتباريين كالدولة والمؤسسات والشركات، ولتلك الجهات بياناتها الخاصة التي تكون البيئة الرقمية موطنها. ولكن لا يطلق على تلك البيانات صفة الشخصية، كون هذه الصفة حصرية بالأشخاص الطبيعيين فقط[2]. لذلك يسبغ على البيانات طابع أو صفة الشخصية، متى ما تعلقت بشخص حي، ولا ينطبق الحال على الأشخاص المتوفين، رغم وجود التأثيرات التي تطال ذويهم من الأحياء.

الفرع الثاني: البيئة الرقمية

أحدثت تكنولوجيا المعلومات تأثيرا كبيرا على البيانات الشخصية وتجميعها، فقد أضحى الانتشار الواسع لجمع تلك المعلومات مسألة لا تحتاج إلى التحقق والتدقيق، ويتم إيداع أوتخزين تلك المعلومات في عدة أماكن وتطبيقات للويب وشبكات الإعلان ومنصات التواصل، منها ما يتم برغبة ومسعى الفرد من تلقاء نفسه، وقد يكون إعطاء تلك البيانات من متطلبات الحياة والعمل والمنافسة، ولكن الصورة المستجدة في عالم اليوم، هي انتهاج الكثير من الدول في تعاملاتها نهج الحوكمة الإلكترونية، وعليه أصبحنا تحت واقع الانصياع للانخراط في البيئة

([1]) المادة (4-1) من اللائحة العامة لحماية البيانات GDPR.

([2]) مادة (2-أ) من التوجيه الأوروبي رقم 46/95 الصادر بتاريخ 1995/10/24.

الرقمية، ولكافة الفئات العمرية، متعلمين أو الأقل تعلما. فلغرض الحصول على الضمان والرعاية الصحية أو التقدم للوظائف – حكومية أو قطاع خاص– ودفع الفواتير على تنوعها، وشراء العقارات والسيارات وما سواها، والحصول على إجازات السوق والبناء، والحصول على تراخيص ممارسة المهن، وغير ذلك الكثير من الحاجات على مختلف الأصعدة، لا مناص من التقدم إلى مختلف المنصات الرقمية بالبيانات الشخصية المتباينة النطاق والتنوع.

ومفهوم البيئة الرقمية يعني المجال الافتراضي الذي يمكن الوصول إليه عبر الإنترنت، والذي يسمح للمستخدمين بالتفاعل مع الآخرين بنشاطات ومجالات متنوعة، مستخدمين وسائل مختلفة، مثل منصات التواصل الاجتماعي أو تقنيات الواقع الافتراضي. ويكون للفرد بصمته الرقمية، من خلال الأدلة والسجلات التي تشير إلى تفاعل الفرد مع البيئة الرقمية.

أما مكونات البيئة الرقمية فتشمل أجهزة التقنية كالحواسيب والهواتف الذكية، والبرامجيات التعليمية، أما الإنترنت فيعد الركن الأساس لبلوغ المحتوى الرقمي. وتتميز بخاصية انعدام الوجود المادي الحسي أو الملموس، حيث يصعب التحكم أو السيطرة عليه، بخلاف بيئة العمل التقليدية الورقية. وتوفر هذه البيئة كما هائلا من المعلومات، مع سهولة الوصول إلى المعلومة من جهة طالبها، وسهولة الطرح وسرعة الانتشار.

أخذت الدول باعتماد السياسات والبرامج التعليمية الحديثة في سياساتها وخططها التعليمية للوصول إلى أعلى مستوى للكفاءة الرقمية لمواطنيها، وبالتالي تحقيق شعار محو الأمية الرقمية، في الوقت الذي سبق ذلك التوجه، الغزو الذي حققته البيئة الرقمية في الوسط الاجتماعي البشري، حيث تسللت بنسب متفاوتة إلى مختلف مكونات المجتمع، بعد أن حجزت مكانها وسط تلك الشرائح كل حسب ثقافته وعمله وتوجهه.

الفرع الثالث: التعدي على البيانات الرقمية للأفراد

من الثابت في عالم اليوم الذي تتسيده تقنية المعلومات الرقمية، والتي أصبحت الحاضن لكثير من المعلومات والبيانات الشخصية للأفراد، أن تلك البيانات تكون عرضة لإساءة الاستخدام بطرق شتى ومن قبل جهات عدة. فما هي تلك الممارسات، ومن هي الجهات الأكثر تعرضا لتلك البيانات؟

أولاً: حالات انتهاك الخصوصية الرقمية

تعد عملية تجميع البيانات الشخصية في البيئة الرقمية من أهم المراحل التي يتعرض فيها الفرد لانتهاك حقه في الخصوصية، خاصة عندما تحدث تلك الممارسات على نطاق واسع([1]). إضافة إلى مراقبة اتصالاته واعتراضها، حيث إن الأصل أن تتم المراسلات والاتصالات وانتقال البيانات إلكترونيا عن طريق الإنترنت بحرية بين المرسل والمرسل إليه. فتتبع تحركات الفرد عبر الإنترنت ومنصاته أو مراقبة اتصالاته يشكل أخطر صور التعدي على خصوصية البيانات.

([1]) لائحة الجمعية العامة للأمم المتحدة المرقمة A/RES/68/167 بتاريخ 2014/1/21 المتعلقة في "الخصوصية في العصر الرقمي"، الدورة 68.

ولكي يكون الاعتراض واقعا ضمن إطار المنع، يتوجب أن يتم التعرض لفئة من البيانات يطلق عليها "البيانات التوصيفية"([1])، وهي طائفة البيانات التي تعكس هوية الفرد وسلوكياته وعلاقاته الاجتماعية، وهو ما يتم التوصل إليه نتيجة جمع وتحليل البيانات، للوصول إلى معرفة دقيقة لتفاصيل الحياة الخاصة للأفراد. ولا ينتفي العمل غير المشروع إن لم يتم استخدام تلك البيانات أو حتى عدم الاطلاع عليها، فمجرد جمع البيانات وتخزينها يعد تعديا على الخصوصية الرقمية للأفراد([2]).

ففي مرحلة التقديم على عمل معين، توجد برامج حوسبة يتم إدخال معلومات موسعة عن طالب العمل، قسم منها متعلق بحياته الخاصة، كالزواج والمعتقد والحالة العاطفية والانتماء، ليتم التحليل الإلكتروني للمعطيات من البيانات الشخصية، وبناءً على الصورة المتبلورة من جمع بيانات صاحب الطلب، يتم الاختيار إلكترونيا بواسطة البرامج المعدة لهذا الغرض([3]).

كما أن البيانات الشخصية التي تكون عرضة للتجميع والانتهاك قد تكون اسمية، حين تتعلق بالوضع العائلي أو الحالة الصحية أو المادية أو الوضع الوظيفي، وهذه معلومات تبين المفاصل الخاصة بالفرد وحياته. وقد تكون البيانات ذاتية معبرة عن آراء الشخص وانتماءاته، سواء تعلقت بشخوص أم قضايا وشؤون معينة. أما البيانات الموضوعية فهي التي تبين موطن الفرد أو وظيفته.

ويشكل الاختراق صورة لانتهاك البيانات الشخصية، ولا تقتصر صوره على الاطلاع أو الاستخدام، بل قد تلجأ الجهة التي تقوم بهذا العمل إلى تدمير حواضن البيانات الشخصية من الحواسيب وأقراص خزن البيانات وأجهزة الاتصال. وبذات الضرر تقوم الجهات بعمليات الاختراق بغرض التلاعب بالبيانات وتغييرها لغايات مختلفة. وهناك صورة تبنى على الاختراق، وهي عمليات التجسس، حيث يتم رصد أنشطة الأفراد من خلال الإنترنت([4]).

ومحور حالة الانتهاك للخصوصية الرقمية يتمحور حول الاطلاع على البيانات ونقلها إلى جهات وأطراف أخرى أو المعالجة وتكوين قواعد بيانات، وتتم تلك الحالات بدون موافقة الشخص المعني أو دون مسوغ قانوني، ومسرح أحداث تلك العمليات وحالة الحدوث تقع في بيئة رقمية، وباستخدام وسائل إلكترونية مستفيدين من التقدم التقني المعاصر، ويتم تجميع البيانات أو تكون محفوظة على قواعد بيانات وسجلات إلكترونية([5]).

وتتلخص حالة انتهاك البيانات الشخصية رقمياً عند الجمع والتخزين والنقل إلى الغير، فبيانات عملاء البنوك تتسم بالسرية، ما يشكل إفشاؤها إحدى صور انتهاك الخصوصية. ويكمن التصرف غير المشروع من ناحية

([1]) الفقرة 19 من الوثيقة A/HRC/27/37 بتاريخ 30 حزيران 2014، تقرير مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي.

([2]) الفقرة 20 من الوثيقة A/HRC/27/37 بتاريخ 30 حزيران 2014، تقرير مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي.

([3]) محمد دياب صالح، الحماية القانونية للحياة الخاصة وضماناتها في ظل الوسائل التكنولوجية الحديثة، دار الكتب القانونية، مصر، 2010، ص 50.

([4]) عاطف كريم، الخصوصية الرقمية بين الانتهاك والغياب التشريعي، مركز دعم لتقنية المعلومات، القاهرة، 2013/20/28، ص 2.

([5]) المادة (3) من اتفاقية بودابست لسنة 2001، والمتعلقة بمكافحة الإجرام المعلوماتي.

الوسائل المستخدمة للحصول على تلك المعلومات، أو في محتوى المعلومات ذاته. فركن العمل المادي يقع في المعالجة خارج إطار القانون، أو باستخدام الوسائل المحظورة في جمع وحفظ البيانات. أما الركن المعنوي، فينتج عن علم وإرادة أو تقصير وإهمال. وقد يعطي صاحب البيانات الموافقة باستخدامها، ولكن هذا الاستخدام يصبح غير مشروع إن تم خارج المدة المحددة أو بعد سحب الموافقة.

ثانياً: الجهات التي تنتهك الخصوصية الرقمية

1-الدول: كثيراً ما تفرض الدول على شركات الاتصالات والمعلوماتية تزويدها ببيانات الأشخاص الذين يستخدمون شبكاتها، كذلك تستعين الدول بأحدث البرامج الإلكترونية المتطورة بهدف الولوج إلى الأجهزة الإلكترونية الخاصة بالأفراد، والحصول على البيانات المتوافرة عليها. كذلك تشهد اتفاقيات التعاون الأمني بين الدول خرقاً للخصوصية الرقمية، بواسطة تبادل بيانات الأشخاص بين الدول الأطراف دون علم أصحابها([1]).

كذلك مكنت التقنيات الحديثة الدول من مراقبة تحركات الأشخاص بواسطة اعتراض مكالمات الهاتف المحمول، أو الدخول غير المشروع للبريد الإلكتروني. كما تخضع الدول نشاطات الأفراد على شبكة الإنترنت للمراقبة، وتستطيع بذلك تحديد الأشخاص الذين يمارسون حرية التعبير بقضايا وشؤون تهم الدولة، ما يرتب عليه كشفا للخصوصية، إضافة إلى الإجراءات التعسفية أو القمعية التي تلحق بالشخص الهدف([2]).

2- شركات تكنولوجيا المعلومات: تعد تلك الشركات على اختلاف نطاق نشاطاتها، محليا أو إقليميا أو عالميا، الجهة الأكثر انتهاكاً لخصوصية الأفراد الرقمية. فتارة تلجأ الدول إلى الضغط على تلك الشركات، بشكل قانوني أو غير قانوني، لتزويدها ببيانات ومعلومات تخص أفرادا محددين أو بشكل عشوائي، وبأعداد قد تصل إلى ملايين البشر. كما قد يقع العمل المحظور من جانب الشركات عند تصميم برامج وتقنيات المراقبة، التي تستخدمها الدول فيما بعد، ومن دون رقابة أو علم أو سيطرة لتلك الشركات. وهذا لا يبرئ ذمة الشركات، فهي مسؤولة عن صون وحماية البيانات التي بحوزتها، أو البرمجيات التي تصممها، ويقع على عاتقها بذل الحيطة والحذر والعناية اللازمتين([3]).

وهناك جملة من الواجبات التي تقع على عاتق المؤسسات والشركات التجارية، مثل شركات تقنيات التواصل الاجتماعي، ومنها؛ إعلام وتنبيه مستخدميها بالمخاطر التي قد تلحق بهم جراء وضع بياناتهم على تلك المنصات، وبطريقة تسهل عليهم الوصول والاطلاع وفهم تلك التحذيرات([4]). ووضع مبدأ الحق في الخصوصية في المقام الأول عند جمع ومعالجة واستخدام البيانات الشخصية، والعمل على منع أو تقليل الانتهاكات الحاصلة جراء

([1]) تقرير المقرر الخاص المعني بالحق في الخصوصية، مجلس حقوق الإنسان، الملحق رقم A/HRC/31/64 في 2016/11/24، ص9.

([2]) تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير، الملحق المرقم A/HRC/23/40، بتاريخ 14 نيسان 2013، ص 12.

([3]) الوثيقة رقم A/HRC/27/37، تقرير مفوض الأمم المتحدة السامي لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، في 30 حزيران 2014، ص 16.

([4]) الوثيقة رقم A/RES/75/176، قرار الجمعية العامة للأمم المتحدة 176/75، الحق في الخصوصية في العصر الرقمي، في 2020/12/16.

عملياتها، من خلال إبلاغ جهات الرقابة عن الحالات التي تحدث، والعمل على بذل أقصى الطاقات والجهود نحو الوصول إلى تقنيات برمجية تساعد على إخفاء الهوية، وتوفير السرية في الاتصالات وتبادل المعلومات([1]).

كما تقوم شركات التجارة الإلكترونية بمعاملة الأفراد كمورد مالي ضخم، مستغلة رغباتهم وحاجاتهم وما يقدم لهم في منصات ومواقع إلكترونية من سلع وخدمات، مقابل قيامهم بإعطاء بيانات شخصية، ليتم جمعها ومعالجتها وتكوين صورة نمطية عن سلوكيات ورغبات الشخص المعني أو حالته الصحية، ليتم الاستهداف من قبل ذات الشركات، أو بيع معلوماته لشركات أخرى، تستفيد من التشخيص المباشر لحاجات الأفراد، ومن ثم تصنيفهم إلى فئات بهدف عرض الإعلانات التي تتضمن سلعا وخدمات وجدت طريقها المباشر للمستهلك من خلال كشف بياناته([2]).

ويتم جمع المعلومات الشخصية للأفراد، إما مباشرة من خلال إعطائه لبياناته التي تطلبها منه المنصات الإلكترونية أو زيارته لمواقع معينة وتتبع حركاته واهتماماته، أو بصورة غير مباشرة من خلال نظام تحديد الموقع أو المعرفات الرقمية للأجهزة التي يستخدمها للولوج إلى شبكة الإنترنت. لتأتي بعد ذلك عملية المعالجة ودمج تلك المعلومات وعمل قاعدة بيانات، أو نقل تلك المعطيات إلى أطراف ثالثة.

المطلب الثاني

الحماية الدولية لبيانات الأفراد الرقمية

حق الإنسان في الحرية وصون الكرامة حق مقدس ومحمي بموجب القانون الدولي لحقوق الإنسان، ويمثل الحق في الخصوصية تجسيدا لتلك الحقوق([3])، حيث يحظر التدخل القسري بشؤون الإنسان وأفراد أسرته ومراسلاته وشن الحملات التي تستهدفه من حيث الشرف والسمعة، وكرس القانون الدولي حق الإنسان على دولته توفير الحماية في حال تعرضه لمثل تلك الممارسات[4]. ويشكل حق الإنسان في حماية بياناته الشخصية عنصرا أساسيا من عناصر الحق في الخصوصية[5]. ويشمل نطاق الحماية الدولية البيانات البيومترية، التي يستطاع من خلالها تحديد هويات الأشخاص، والبيانات الجينية، وطائفة البيانات الشخصية المتعلقة بالإدانة والجرائم والاحترازات الأمنية([6]).

([1]) الوثيقة رقم A/HRC/34/7، قرار مجلس حقوق الإنسان 7/34، الحق في الخصوصية في العصر الرقمي، في 7 نيسان 2017.

([2]) المادة (4-4) من اللائحة العامة لحماية البيانات المرقمة 679/2016.

([3]) الفقرتين (50-51) من الوثيقة A/HRC/40/63 بتاريخ 2019/10/16، تقرير المقرر الخاص المعني بالحق في الخصوصية، الحق في الخصوصية، الدورة الأربعون. كذلك، المادة 8 من الاتفاقية الأوروبية لحقوق الإنسان، المادتان 16 و 21 من الميثاق العربي لحقوق الإنسان، المادة 16 من اتفاقية حقوق الطفل.

([4]) المادة (12) من الإعلان العالمي لحقوق الإنسان، المعتمد بموجب قرار الجمعية العامة للأمم المتحدة 217 ألف (د-3)، بتاريخ 1948/12/12. والمادة (17) من العهد الدولي للحقوق المدنية والسياسية، المعتمد بموجب قرار الجمعية العامة للأمم المتحدة 2200 (د-21)، تاريخ 1948/12/16.

([5]) نصت على هذا الحق المواثيق الإقليمية والدولية، وكذلك القوانين الداخلية لغالبية الدول.

([6]) المادة 6 من اللائحة العامة لحماية البيانات، وتمثل قانون حماية البيانات الشخصية الأوروبي.

وسنبحث في الفرع الأول، المسؤولية التي تقع على عاتق الدول تجاه حق الفرد في خصوصية بياناته الشخصية في البيئة الرقمية، أما الفرع الثاني، فسيسلط الضوء على حدود حق الأفراد في خصوصيتهم الرقمية.

الفرع الأول: مسؤولية الدول بضمان الحماية

أولاً: الحماية التشريعية

وجهت الجمعية العامة للأمم المتحدة الدول الأعضاء بالوفاء بتعهداتها من جهة الالتزام بمفاعيل الحق في الخصوصية، الذي يتضمن حق الفرد في احترام خصوصية بياناته الشخصية. وتنفيذ تلك الالتزامات تتطلب من الدول اتخاذ ما يلزم من إصدار تشريعات متوافقة مع أحكام القانون الدولي لحقوق الإنسان([1])، تكفل تمتع الفرد بصون سرية بياناته الشخصية، وعدم استخدامها بغير إذنه أو علمه إلا في أضيق الحدود، وبما يتطابق مع التشريعات الداخلية ومقتضيات القانون الدولي، وتحقيق المصلحة العامة([2]).

في حين شدد مجلس حقوق الإنسان، بأن على الدول العمل على إقرار وإنفاذ القوانين التي تضمن حماية البيانات الشخصية للفرد، ونطاق الالتزام بحرمة التعدي على الخصوصية الرقمية يشمل القطاعين العام والخاص، ويجب أن تضمن كفالة تلك الحماية بجزاءات تلحق بالمخالفين([3]). مع ضرورة قيام الدول بمراجعة التشريعات والإجراءات المتعلقة بجمع البيانات الشخصية ومراقبة الاتصالات واعتراضها، بغية التأكد من تطبيق مضامين الحق في الخصوصية في مختلف الأوقات([4]).

فمسؤولية الدول تنبع من حيث كونها طرفاً في اتفاقية دولية موضوعها حماية الحق في الخصوصية، وكذلك تلتزم الدول بأحكام بعض الاتفاقيات التي تحولت أحكامها إلى قواعد عرفية واجبة التطبيق([5]). ورغم ذلك فهناك حاجة فعلية لوضع أطر دولية ملزمة تأخذ بعين الاعتبار التقدم التقني الحاصل وأثره على مفهوم الحق في الخصوصية الرقمية([6]).

ثانياً: الحماية القضائية

تكفل الدولة توفير وتسهيل سلوك طرق المراجعة القضائية أمام الأفراد الذين تعرضوا لانتهاك بياناتهم الرقمية، حيث يستطيع الفرد مقاضاة أجهزة الدولة المسؤولة عن تلك الانتهاكات، من خلال اتخاذها القرارات

([1]) الفقرة (4–ب) من الوثيقة A/RES/68/167 بتاريخ 2014/1/21، لائحة الجمعية العامة للأمم المتحدة.

([2]) الفقرة (4–ج) من الوثيقة A/RES/68/167 بتاريخ 2014/1/21، لائحة الجمعية العامة للأمم المتحدة.

([3]) الوثيقة A/HRC/48/31، تقرير مفوض الأمم المتحدة السامي لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي، في 13 أيلول 2021، ص 19.

([4]) رشيدة بوكرة، تحديات العصر الرقمي في مواجهة خطط حماية الحق في الخصوصية، مجلة حقوق الإنسان والحريات العامة، مجلد 7، العدد 2، 2022، ص 81–82.

([5]) رزوق سلمودي وآخرون، الموقف المعاصر للقانون الدولي العام من الحق في الخصوصية في العصر الرقمي، المجلة العربية الأمريكية للبحوث، المجلد 3، العدد 2، 2017، ص 9.

([6]) الوثيقة (الملحق) A/RES/73/179، الصادرة بقرار الجمعية العامة للأمم المتحدة179/73، بعنوان الحق في الخصوصية في العصر الرقمي، تاريخ 2019/1/21.

وإصدارها لأوامر أفضت إلى جمع أو نقل البيانات الشخصية أو مراقبة واعتراض منافذ التواصل من اتصالات ومخاطبات أو محادثات. وهذا ما يتطلب التعامل بشفافية من قبل الجهات المستقلة المحلية، سواء أكانت تشريعية أم إدارية أم قضائية([1]).

وهذا ما يتطابق مع التزامات الدول بموجب العهد الدولي الخاص بالحقوق المدنية والسياسية، الذي ألزم الدول بتوفير طرق التظلم، إلى جانب كفالة تنفيذ الأحكام الصادرة بهذا الخصوص([2]). ولم يرسم للدولة انتهاج طريق بعينه، بل ترك لها وفق سلطتها التقديرية تحديد الجهات التي تتولى ذلك، سواء كان القضاء الإداري أم العادي. والمهم في الأمر هو فسح الطريق أمام من انتهكت حقوقهم للتظلم وطلب الانتصاف، وتحديد جهات مستقلة مهنية وفق معايير قانونية، تزود بالكوادر والإمكانات المادية والبشرية، وتعطى الحرية في التنقل والوصول إلى المعلومات التي تساعدها في أداء مهامها، وإمكانية إصدار القرارات بدون تأثير من جهات حكومية، مع التشديد على ضرورة الانتصاف عبر القضاء وعدم الاكتفاء بالتعويض خارج إطار المؤسسة القضائية([3]).

وتظهر أهمية الحق في حماية البيانات الشخصية في التحقيقات الدولية التي تستخدم تقنيات الاتصالات الرقمية وشبكة المعلومات العنكبوتية. فالمحققون الدوليون في انتهاكات القانون الدولي الإنساني وقانون حقوق الإنسان يجب أن يكونوا على دراية كافية وفهم للقوانين المتعلقة بالحق في الخصوصية وحماية البيانات، ففي عمليات الرصد التي يقوم بها المحققون من أجل الحصول على بيانات عامة، وإن كانت مجهولة المصدر، قد يفضي الكم الهائل من المعلومات إلى الكشف عن هوية صاحب العلاقة، في حال مقارنتها أو جمعها مع بعضها، أو مقارنتها ببيانات أخرى منشورة[(4)].

كذلك تثير حالات استمرارية رصد الأفراد على الإنترنت وتجميع البيانات الشخصية بشكل منتظم ولفترات ممتدة، القلق من احتمالية خرق تلك الأنشطة للقوانين التي تحمي البيانات الشخصية[(5)]. حيث يحظر جمع المعلومات إلا لأغراض مشروعة ومحددة وصريحة، مع قصرها بالغرض الذي جمعت من أجله وللفترة اللازمة لذلك[(6)].

كذلك نجد الحماية الدولية للحق في سرية البيانات الشخصية من خلال القضاء الدولي، حيث ينظر إلى الخصوصية بأنها تعزيز لكرامة الإنسان والقيم والحريات الأساسية، كحرية التعبير وحرية تكوين الجمعيات، فيتلمس

([1]) الفقرة (4-د) من الوثيقة A/RES/68/167 بتاريخ2014/1/21،لائحة الجمعية العامة للأمم المتحدة.

([2]) الفقرة (12) من التعليق العام رقم (31) للجنة المعنية بحقوق الإنسان في دورتها ال80 سنة 2004، بعنوان "طبيعة الالتزام القانوني العام المفروض على الدول الأطراف في العهد".

([3]) الفقرة (41) من الوثيقة A/HRC/27/37، تقرير مفوضية الأمم المتحدة السامية لحقوق الإنسان: الحق في الخصوصية في العصر الرقمي، بتاريخ 30-6-2014.

([4]) John Czajka and others, Minimizing Disclusure Risk in HHS Open Data Initiatives (Washington, D.C., Mathematica Policy Research, 2014), appendix E, P. E-7.

https//:aspe.hhs.gov/system/files/pdf/77196/rpt_Disclusure.pdf Last Visit 2 May 2025

([5]) المادتين (5) و (6) من اللائحة 679/2016 الصادرة عن البرلمان الأوروبي والمجلس بتاريخ 27 نيسان 2016 الخاصة بحماية الأشخاص الطبيعيين فيما يخص معالجة البيانات الشخصية وحرية حركة تلك البيانات.

([6]) الفصل (2) من قانون حماية البيانات لعام 2018، الجزء 3، الفصل (3)، القسم 39 (1). المملكة المتحدة لبريطانيا العظمى وأيرلندا الشمالية.

الدفاع في انتهاك حرمة البيانات الشخصية طريقاً للطعن في سلامة الإجراءات الجنائية، وحقا لطلب التعويض من خلال إقامة الدعاوى المدنية بحق أطراف التحقيق[1]. كما يحظر النفاذ إلى البيانات الشخصية عن طريق الخداع الذي يعد أحد أشكال الهندسة الاجتماعية[2].

ثالثاً: رقابة البيانات الرقمية والاتصالات

قيدت العديد من القرارات الصادرة عن الجمعية العامة للأمم المتحدة ومجلس حقوق الإنسان([3])، سلطة الدولة في تتبع ومراقبة بيانات الأشخاص واتصالاتهم الرقمية، في إطار حماية أمن الدولة أو مكافحة الإرهاب أو الجرائم الدولية. حيث خلصت تلك القرارات إلى التطابق في المضامين والمخرجات للحق في الخصوصية وضرورة حمايته في البيئة الرقمية أسوة بالبيئة المادية أو الطبيعية خارج الإنترنت، التي كانت ماثلة في أذهان واضعي الإعلان العالمي لحقوق الإنسان. ومن ثم، فإن الجهود المبذولة في تحقيق الأمن على صعيد التكنولوجيا يجب أن لا تكون بهدر حقوق الإنسان المعترف بها في المواثيق الدولية.

كما انتهجت الأمم المتحدة ضمن تشكيلاتها وأجهزتها ذات السياسة في نطاق عملها، راسمة بذلك جملة من المبادئ. حيث تقوم على تنسيق المعايير المتعلقة بحماية البيانات الشخصية بين الأجهزة أو الوكالات، مع تسهيل عمليات معالجة تلك البيانات([4]).

كذلك اعتمدت منظمة اليونسكو جملة من المبادئ تعنى بحماية البيانات الشخصية، مؤكدة على ضرورة التحديد الدقيق لأغراض المعالجة والضرورة التي تستدعي المعالجة لتحقق الغرض وحصر عمليات المعالجة بحدود ما تتطلبه حالة الضرورة، مع مراعاة التوازن بين تلك الأغراض والحقوق والحريات. واتخاذ التدابير التقنية والإدارية لضمان أمن البيانات من أن يتم الاطلاع عليها بطريقة عرضية، أو فقدانها. كما يجوز نقل البيانات إلى طرف مكلف بمهام نيابة عن الطرف المصرح له، شريطة الالتزام بحماية تلك البيانات([5]).

([1]) المادة (69) الفقرة (7) من نظام روما الأساسي. كذلك تنص اللائحة 679/2016 الصادرة عن البرلمان الأوروبي والمجلس بتاريخ 27 نيسان 2016 بشأن حماية الأشخاص الطبيعيين فيما يتعلق بمعالجة البيانات الشخصية وحرية حركة تلك البيانات على أن الأشخاص الطبيعيين يتمتعون بحقوق مرتبطة بحماية البيانات الشخصية وحماية معالجة البيانات الشخصية وحركة البيانات الشخصية غير المقيدة داخل الاتحاد الأوروبي. كما تنص اتفاقية حماية الأفراد فيما يتعلق بالمعالجة الآلية للبيانات الشخصية على حقوق مماثلة، ولا سيما بروتوكول 2018 الملحق بها. ولا تلزم الاتفاقية الدول الأعضاء في مجلس أوروبا فحسب، بل عدداً من الدول الأخرى.

([2]) الهندسة الاجتماعية هي " فعل خداع شخص لحمله على كشف معلومات حساسة عبر التواصل معه لكسب الثقة".

Paul A. Grassi, Michael E. Garcia and James L. Fenton, Digital Identity Guidelines, Gaithersburg, Maryland, National Institute of Standards and Technology, 2017, p.54.

([3]) الوثيقة A/RES/68/167 من قرار الجمعية العامة 168/67، الحق في الخصوصية في العصر الرقمي، في 2013/12/18. و الوثيقة A/HRC/32/L.20k، قرار مجلس حقوق الإنسان 32/13، تعزيز وحماية حقوق الإنسان على الإنترنت والتمتع بها، 27 حزيران 2016.

([4]) مبادئ حماية البيانات الشخصية والخصوصية، والمعتمدة من قبل اللجنة الإدارية الرفيعة المستوى التابعة للأمم المتحدة(HLCM) في اجتماعها ال36 بتاريخ2018/10/11.

([5]) اعتمدت من قبل اللجنة العليا للإدارة في الاجتماع الـ 36 المنعقد بتاريخ 11 تشرين أول 2018.

رابعاً: الهيئات الرقابية

سنت العديد من الدول مختلف التشريعات، سواء ما تعلق منها بوضع الخصوصية أم بغيره، تحظر سلوكيات معينة. لكن وجود تلك التشريعات، التي تعنى بحماية البيانات الرقمية، في نظر الأمم المتحدة، لا تعد ضمانة حقيقية لصون تلك الحقوق من التعدي. لذا، تتطلب مسألة إحكام تلك الحماية وجود هيئات رقابية مستقلة، تكون مهمتها رصد حالات انتهاك خصوصية الأفراد الرقمية، وتمتلك من الإمكانات البشرية والتقنية ما تستطيع من خلاله القيام بدورها على أكمل وجه.

حيث تزود تلك الهيئات بصلاحيات وفق آليات تستطيع من خلالها مراقبة الخروقات الحاصلة، سواء من القطاع العام أم الخاص، والتحقق من البلاغات والشكاوى التي تصلها بهذا الخصوص، وإصدار الجزاءات المناسبة، والتي تحقق عملية الردع والزجر([1]). إلا أن التحديات والصعوبات التي تواجه تلك الضمانة كبيرة، سواء من جهة الاصطدام بسلطة الدولة وهيمنتها، أم من جهة الخروقات ذات الطابع العابر للحدود، وتشعب وتعقد العمليات التي تنتهك حق الخصوصية.

خامساً: عدم إساءة استخدام البيانات

يتطلب الحصول على خدمة أو عمل تقديم بيانات للجهة المشغلة أو المزودة بالخدمة، وفي عالم اليوم تتخذ تلك العملية من التطبيقات والأرشفة الإلكترونية طريقاً لها. لذا، وحرصاً على ضمان حصر تلك العمليات بالغرض الذي طلبت من أجله تلك البيانات، لا يجوز الاحتفاظ بها لفترات تجاوز الحاجة الفعلية التي من أجلها جمعت([2])، مع تمكين صاحب تلك البيانات من الوصول إليها والاطلاع على تفاصيلها، والاحتفاظ بحقه في الحذف والتعديل، كما تجدر الإشارة إلى عدم جواز جمع معلومات غير متعلقة مباشرة بالعمل أو الخدمة المطلوبة. كتفاصيل الحالة الصحية للعامل أو الحالة الزواجية أو العاطفية أو محل السكن، ما لم يكن ذلك مرتبطا ارتباطا مباشرا بطبيعة ومتطلبات العمل([3]).

وأكدت المفوضية السامية لحقوق الإنسان على اعتماد أنظمة وتطبيقات الذكاء الاصطناعي بشكل أساسي على كم هائل من بيانات ومعلومات الأفراد، من خلال جمعها ومعالجتها وتحليلها([4])، فهي أساس ومحور عمل تطبيقات الذكاء الاصطناعي، حيث يتم تغذيتها بتلك البيانات، التي في بعض الأحيان تكون قديمة أو تمييزية أو معيبة، ومن خلال معالجة بيانات الفرد المتعلقة بهواياته وتفضيلاته وسلوكه وعلاقاته الاجتماعية، تكمن مخاطر

([1]) الوثيقة رقم A/RES/69/166، قرار الجمعية العامة للأمم المتحدة 166/69، الحق في الخصوصية في العصر الرقمي، في 2014/12/18.

([2]) باشيليت، مخاطر الذكاء الاصطناعي التي تهدد الخصوصية تتطلب اعتماد إجراءات عاجلة، 15 أيلول 2021، على الرابط www.ohchr.org/ar/press-releases/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet.

آخر زيارة في 6 أيار 2025

([3]) المادة (4-ج) من الاتفاقية رقم (179) بشأن تعيين وتوظيف البحارة والمعتمدة من قبل مؤتمر العمل الدولي في دورته (84) في حزيران 1984م.

([4]) المعالجة هي عملية أو مجموعة من العمليات التي تجري على البيانات الشخصية أو مجموعة منها، بأي وسيلة كانت تقليدية أو إلكترونية، مثل الجمع أو التنظيم أو التسجيل.

تطال الحق في الخصوصية، إذا ما استغلت في الكشف عن التنبؤ السلوكي أو التنميط للفرد أو تحديد هويته من خلال التعرف على الوجه بايومتريا أو تتبعه([1]).

كما أن هناك آليات ووسائل تساعد على تعزيز حماية البيانات الشخصية، منها مراجعة واستعراض الممارسات والسياسات التي تنتهجها الحكومات بشأن جمع البيانات الشخصية واعتراض الاتصالات الرقمية، بغية تحديد التدابير التي تعد انتهاكا للخصوصية. وكذلك تتحمل مؤسسات القطاع الخاص مسؤولياتها تجاه احترام خصوصية البيانات الرقمية للأفراد.

وفي حقيقة الأمر، وبالرغم من تأكيد المنظمات الدولية ورسمها لحدود حقوق الأفراد في حماية بياناتهم الشخصية، إلا أن المتتبع لممارسات الدول والشركات العالمية المالكة للمنصات الرقمية، يجد أنها لا تزال تمارس سياسة الاستغلال والتعدي على تلك الحقوق، وليس أقلها ما حدث في عملية انتخابات الرئاسة الأمريكية عام 2018م، وما دار حولها من اختراق لبيانات عشرات الملايين من الناخبين. وكذلك تلجأ الشركات العالمية، مثل فيسبوك ومنصة أكس (تويتر سابقا)، لابتزاز الدول بتهديدها بقطع خدماتها عنها في حال فرض غرامات أو تعويضات على انتهاكاتها لقوانين حماية الخصوصية.

ويجدر التساؤل هنا، في أوقات جائحة كورونا، تم جمع بيانات أعداد ضخمة من الأفراد، ولأسباب تتعلق بالظروف الطارئة في حينها. فهل تم استغلال تلك الحاجة من قبل الدول والشركات لأغراض أخرى، وهل تم تجهيل هوية أصحابها، وهل لا تزال بياناتهم مدرجة على أرشيف تلك المنصات، أم تمت إزالتها تماشيا مع مبادئ الغائية والتقييد الزمني.

الفرع الثاني: حدود الحق في الخصوصية

رغم تأكيد العديد من المواثيق الدولية على ترسيخ هذا الحق وحظر إهداره، إلا أن هذا الحق ليس بالحق المطلق، حيث يجوز لسلطات الدولة تقييد هذا الحق، والتدخل في خصوصية الأفراد عند توافر ظروف معينة وبشروط ومحددات لسلطة الدولة في هذا الخصوص.

ولكي يكون تصرف الدول ضمن نطاق الشرعية، لا بد أن يستند هذا التدخل إلى نص تشريعي يجيز ذلك التصرف، وضروة أن تتسم صياغة تلك الأحكام بالوضوح والشفافية، والابتعاد عن كل ما من شأنه أن يؤدي إلى تأويلات أو غموض في الدلالة والتفسير([2]). وحتى في حال إسناد حالات التدخل في الخصوصية لسلطة القانون، فلا مناص من التأكد من مراعاة القوانين المحلية لأحكام العهد الدولي للحقوق المدنية والسياسية([3]). ويتضمن نص

([1]) عمرو وجدي، الذكاء الاصطناعي والحق في الخصوصية، 5 آذار 2023، آخر زيارة 1 أيار 2025 على الرابط https://www.shorouknews.com/mobile/columns/view.aspx?cdate=05032023&id=efb9ca3c-ve5a-4260-8a68-e6af103f70b1.

([2]) Privacy Internationl, Guide to International Law and Surveilliance, viewed on 05/05/2025 https://privacyinternational.org/sites/default/files/2017-12

([3]) التعليق العام رقم (16) للجنة المعنية بحقوق الإنسان.

القانون تبيان للحالات التي يرخص فيها اللجوء لهذا الاستثناء، والجهات المخولة بمباشرة تلك السلطات، بحيث يكون الأفراد على علم مسبق بهذا الاستثناء وملابساته.

يضاف إلى عنصر الشرعية حالة الضرورة، وهي المبرر الموجب لتقييد الحق في الخصوصية، ومفاده أن هناك حاجة ملحة تستوجب تعطيل هذا الحق، وأن لا سبيل أمام السلطة لاستدراك الضرورة التي حتمت هذا التصرف سوى الاطلاع على البيانات الشخصية للفرد، وضرورة محدودية معالجة البيانات على القدر والسبب الذي استوجب ذلك الاستثناء. كما يتوجب إثبات العلاقة السببية بين الظروف الموجبة لتحديد هذا الحق والفائدة المرجوة من جراء هذا التصرف، شريطة أن لا يقود هذا الإجراء لانتهاك حقوق أخرى للفرد([1]).

وتشرع سلطات الدول عادة قوانين تبيح لها استثناء التعرض للحق في الخصوصية بناءً على مقتضيات المصلحة أو السلامة العامة، والرفاهية الاقتصادية للبلد أو حماية الحقوق والحريات للآخرين، ومنع تفشي الجرائم أو الحفاظ على النظام العام([2]). ورغم ذلك، من غير المباح لهيئات إنفاذ القانون ممارسة السلطات التقديرية المطلقة عند تقييدها لحق الخصوصية، كون القيود هي استثناء من الأصل، وهذا لا يبيح بأي حال من الأحوال تقييد جوهر الحق في خصوصية البيانات الرقمية للأفراد([3]).

فحالة الموازنة والتناسب شرط أساسي لإباحة التدخل ومعالجة البيانات الشخصية، الذي يقيم المصلحة المتحققة من ذلك، فوضوح الأهداف وتحديدها وعدم الإفراط والمبالغة في استخدام البيانات للتوسع بغايات أبعد مما تتطلبه الحالة المشروعة([4])، يعد قيداً على السلطات في مقاربة هذه الحالات، وهو ما تم بحثه في مسائل محاربة الإرهاب([5]).

ومن جملة التدابير التي تقيد سلطة الدولة في إطار المراقبة واعتراض البيانات الشخصية، وتحاشياً من الوقوع في حلقة إساءة استعمال السلطة، يستلزم لتشريع القوانين التي تعالج الحالات الطارئة التي يقيد فيها الحق في خصوصية البيانات الرقمية، أن يتضمن القانون أنواع الجرائم وطبيعتها، وشرائح الأفراد الذين يتطلب معالجة بياناتهم، والمدة الزمنية لذلك الاعتراض، كون إطالة أمد الاحتفاظ ببيانات الأفراد قد يزيد من مخاطر كشف هوية أصحابها، لا سيما في ظل سياسة الدولة في التوسع بعملية تخزين البيانات وجمعها بواسطة شركات مزودي خدمات

([1]) الفقرة (23) من الوثيقة A/HRC/27/37 والمؤرخة في 30 حزيران 2014، تقرير مفوضية الأمم المتحدة السامية لحقوق الإنسان، الحق في الخصوصية في العصر الرقمي.

([2]) الاتفاقية الأوروبية لحقوق الإنسان، روما، 1950/11/4.

([3]) الوثيقة رقم A/HRC/23/40، تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير، في 17 نيسان 2013، ص 10.

([4]) المادة (5-ج) من اللائحة العامة لحماية البيانات.

([5]) الوثيقة رقم A/69/397، مذكرة الأمين العام للأمم المتحدة بشأن تعزيز حقوق الإنسان وحمايتها في سياق مكافحة الإرهاب، في 23 أيلول 2014، ص8.

الإنترنت والاتصالات([1])، ومن هي الجهات المخول لها ذلك، والتدابير والاحتياطات اللازمة لتلك العمليات، حفاظا على سرية البيانات وحمايتها من التلف([2]).

الخاتمة

رغم إقرار الدول بدساتيرها بحقوق الإنسان الأساسية، وحرمة المنزل والمراسلات والحرية والكرامة، إلا أن الواقع يشهد ممارسات تجانب ذلك الالتزام، وما سهل إخفاء بعض من تلك الممارسات هو صعوبة إثبات تلك الخروقات المتعلقة ببيانات الأفراد في البيئة الرقمية الافتراضية. وقد توصلنا من خلال هذا البحث لجملة من النتائج والتوصيات:

أولاً النتائج

1- الحق في الخصوصية بوجهه الحديث (حماية البيانات الشخصية)، يتجلى بحرية الأفراد في السيطرة على حفظ وتنقيل بياناتهم عبر الإنترنت بمنصاته المختلفة.

2- غياب القواعد القانونية الملزمة التي توفر الحماية لبيانات الأفراد الشخصية عالميا، وبما يتناسب مع التطور التقني للمعلوماتية المعاصر.

3- صعوبة الوقوف على الحد الفاصل بين متطلبات تنظيم الحياة الاجتماعية من قبل الدولة وحاجتها في معرفة ما يقتضيه ذلك من التعرف على البيانات، واحترام الحق في خصوصية تلك البيانات المقصورة على أصحابها.

4- وجود إطار قانوني ملزم يحمي البيانات الشخصية على نطاق الاتحاد الأوروبي، متمثل باللائحة العامة لحماية البيانات (GDPR).

5- رغم قيام الدول بسن التشريعات التي تعنى بضمان الحقوق الرقمية للأفراد، إلا أن التطبيق والممارسة يشيان بتحلل الحكومات من وضع نفسها تحت الإطار القانوني لتلك القوانين، بذرائع مختلفة وتفسيرات مطاطة لمبررات مشروعة، كحفظ الأمن القومي أو مكافحة الإرهاب.

ثانياً:التوصيات

1- نشر الوعي العام بمفاهيم الحق في خصوصية البيانات الشخصية، والمخاطر التي تحيق بها، لا سيما تحديات الأمن السيبراني، مع الارتقاء بمستوى التعلم بحيث يمكن الفرد من حماية بياناته على منصات الإنترنت.

([1]) الوثيقة A/HRC/29/32، تقرير المقرر الخاص المعني بتعزيز وحماية الحق في حرية الرأي والتعبير، في 22 أيار 2015، ص 24.

([2])Privacy Internationl, Guide to International Law and Surveilliance,0p.cit.

2- تحديث التشريعات الدولية والداخلية بما يكفل مواءمتها للتطور التقني، مع تفعيل آليات الرقابة والمساءلة عن الخروقات والانتهاكات.

3- العمل على حشد التعاون والتنسيق بين الدول، فيما بينها وكذلك مع المنظمات الدولية، بهدف بلوغ الأمن المستدام في ظل اجتياح المجال الرقمي لمختلف جوانب الحياة حاضرا ومستقبلا، بغية الاستفادة من تقنيات التطور ودرء مخاطرها.

4- جعل حقوق الإنسان في المقام الأول عند الشروع في تصميم أو تطوير أو تنفيذ البرامجيات الرقمية.

5- ضرورة العمل على تصويب أداء الشركات، ولا سيما العالمية منها، التي تعمل على تجميع بيانات الأشخاص، من جهة إبلاغ الأفراد بكل شفافية في سياسة الخصوصية، بأن معالجة بياناتهم لا تخلو من عمليات الخداع والاستغلال، وأنه يتم العمل على تكوين قاعدة بيانات لهم، سوف تستخدم من قبل أطراف ثالثة.

قائمة المصادر والمراجع

أ: المصادر باللغة العربية

أولا: الكتب

- محمد دياب صالح، الحماية القانونية للحياة الخاصة وضماناتها في ظل الوسائل التكنولوجية الحديثة، دار الكتب القانونية، مصر، 2010.

ثانياً: البحوث والمقالات

1. رزوق سلمودي وآخرون، الموقف المعاصر للقانون الدولي العام من الحق في الخصوصية في العصر الرقمي، المجلة العربية الأمريكية للبحوث، المجلد 3، العدد 2، 2017.
2. رشيدة بوكرة، تحديات العصر الرقمي في مواجهة خطط حماية الحق في الخصوصية، مجلة حقوق الإنسان والحريات العامة، مجلد 7، العدد 2، 2022.
3. رؤى سعد القرني، الحماية القانونية للحق في الخصوصية المعلوماتية: دراسة مقارنة، مجلة كلية الدراسات الإسلامية والعربية للبنات، الجزء الأول، العدد 6، 2021، ص1036.
4. عاطف كريم، الخصوصية الرقمية بين الانتهاك والغياب التشريعي، مركز دعم لتقنية المعلومات، القاهرة، 2013/20/28.
5. فطيمة نساخ، حماية الحق في الخصوصية في ظل البيئة الرقمية، المجلة الأكاديمية للبحث القانوني، المجلد 13، العدد 1، 2022.
6. ياسمين بنت نبي بالعسل ، مقدر نبيل، الحق في الخصوصية الرقمية، مجلة المستقبل للدراسات القانونية والسياسية، المجلد 5، العدد 1، 2021.

ثالثاً: الوثائق الدولية

- اتفاقيات دولية.
- وثائق دولية.

رابعا: مواقع الإنترنت

- باشيليت، مخاطر الذكاء الاصطناعي التي تهدد الخصوصية تتطلب اعتماد إجراءات عاجلة، 15 أيلول 2021، على الرابط
www.ohchr.org/ar/press-releases/2021/09/artificial-intelligence-risks-privacy-demand-urgent-action-bachelet.
- عمرو وجدي، الذكاء الاصطناعي والحق في الخصوصية، 5 آذار 2023، آخر زيارة 1 أيار 2025 على الرابط
www.shorouknews.com/mobile/columns/view.aspx?cdate=05032023&id=efb9ca3c-ve5a-4260-8a68-e6af103f70b1.

List of Sources and References

A. Sources in Arabic

First: Books

- Muhammad Diab Saleh. (2010). *Legal Protection of Private Life and Its Safeguards in Light of Modern Technological Means*. Dar Al-Kutub Al-Qanuniyya, Egypt.

Second: Research Papers and Articles

1. Razouq Salmoudi et al. (2017). "The Contemporary Position of Public International Law on the Right to Privacy in the Digital Age." *Arab American Journal for Research*, Vol. 3, No. 2.
2. Rachida Boukra. (2022). "Challenges of the Digital Age in Confronting Plans for the Protection of the Right to Privacy." *Journal of Human Rights and Public Freedoms*, Vol. 7, No. 2.

3. Ru'a Saad Al-Qarni. (2021). "Legal Protection of the Right to Informational Privacy: A Comparative Study." *Journal of the College of Islamic and Arabic Studies for Girls*, Part One, No. 6, p. 1036.
4. Atef Karim. (2013). "Digital Privacy between Violation and Legislative Absence." Information Technology Support Center, Cairo, October 28, 2013.
5. Fatima Nassakh. (2022). "Protection of the Right to Privacy in the Digital Environment." *Academic Journal of Legal Research*, Vol. 13, No. 1.
6. Yasmine Bent Nabi Belassel & Muqaddar Nabil. (2021). "The Right to Digital Privacy." *Al-Mustaqbal Journal for Legal and Political Studies*, Vol. 5, No. 1.

Third: International Documents

- International Conventions.
- International Documents.

Fourth: Internet Sources

- Bachelet. (2021). "Artificial Intelligence Risks Threatening Privacy Require Urgent Action." September 15, 2021. Available at: OHCHR.
- Amr Wagdy. (2023). "Artificial Intelligence and the Right to Privacy." March 5, 2023. Last accessed May 1, 2025. Available at: Al Shorouk News.

English References

1. John Czajka and others, Minimizing Disclusure Risk in HHS Open Data Initiatives (Washington, D.C., Mathematica Policy Research, 2014), appendix E. https//:aspe.hhs.gov/system/files/pdf/77196/rpt_Disclusure.pdf . .2
3. Paul A. Grassi, Michael E. Garcia and James L. Fenton, Digital Identity Guidelines, Gaithersburg, Maryland, National Institute of Standards and Technology, 2017.
4. Privacy Internationl, Guide to International Law and Surveilliance, viewed on 05/05/2025.https://privacyinternational.org/sites/default/files/2017-12