الدراسة الثامنة:
الحقوق الرقمية في عصر الذكاء الاصطناعي والمراقبة الجماعية: منظور قانوني دولي معاصر

د. ربيع طربيه

Abstract

The issue of digital privacy has emerged as a critical and increasingly relevant topic in today's globalized world, shaped by rapid technological advancements and the widespread use of artificial intelligence.

These developments have led to unprecedented expansion in the collection, processing, and surveillance of personal data, posing significant challenges to fundamental human rights. As digital violations intensify and effective oversight remains absent in some countries, the need to reassess legal and regulatory frameworks has become imperative to safeguard individuals from infringements on their privacy, whether by governmental entities or major tech corporations.

Focusing on the intersection between artificial intelligence and the right to privacy provides a profound opportunity to understand the future challenges that societies may encounter. It also underscores the pressing necessity to develop adaptive legislation that ensures the

responsible use of emerging technologies without compromising fundamental rights and freedoms.

By examining the implications of artificial intelligence-driven surveillance and exploring international legal responses, this research aims to shed light on effective strategies to protect digital privacy. In doing so, it advocates for a balanced approach that reconciles technological innovation with the safeguarding of individual liberties.

ملخص

تكتسب قضية الخصوصية الرقمية أهمية متزايدة في العصر الحديث، حيث أصبحت من القضايا المحورية على الصعيدين المحلي والدولي. ويعود ذلك إلى التطور التكنولوجي المتسارع وانتشار تقنيات الذكاء الاصطناعي، مما أدى إلى توسّع غير مسبوق في جمع البيانات الشخصية ومراقبتها. في ظل هذه التحولات، يرتبط الحق في الخصوصية الرقمية ارتباطًا وثيقًا بحقوق الإنسان، التي تُعدّ من الركائز الأساسية في القانون الدولي.

إن تزايد الانتهاكات الرقمية وغياب الرقابة الفعالة في بعض الدول يفرضان ضرورة إعادة النظر في الأطر القانونية والتنظيمية لضمان حماية الأفراد من انتهاك خصوصياتهم. وتشمل هذه الانتهاكات جمع البيانات دون موافقة، واستخدام تقنيات المراقبة الجماعية بما يمسّ بالحريات الأساسية.

من هنا، تبرز أهمية هذا البحث في تسليط الضوء على التحديات القانونية الناشئة عن استخدام الذكاء الاصطناعي في مجال المراقبة الرقمية، واستكشاف السبل الكفيلة بضمان حماية الحق في الخصوصية. إن فهم العلاقة بين التقنيات الحديثة والحق في الخصوصية يمكّن من تحديد المخاطر المستقبلية، ويدعو إلى تطوير تشريعات متقدمة تتماشى مع التطورات التكنولوجية، بما يضمن توازنًا بين الابتكار وحماية الحقوق.

المقدمة

شهد العالم في العقود الأخيرة تطورًا رقميًا غير مسبوق، تجلى في الانتشار الواسع للتقنيات الذكية، وزيادة الاعتماد على شبكات الإنترنت، وتنامي دور الذكاء الاصطناعي في مختلف مجالات الحياة. أسهم هذا التحول الرقمي بشكل كبير في تسهيل التواصل، وتسريع تداول المعلومات، وتحسين جودة الحياة، إلا أنه في الوقت ذاته أفرز تحديات جديدة تمس الحقوق والحريات الأساسية للأفراد، وعلى رأسها الحق في الخصوصية.

لقد أصبحت البيانات الشخصية في العصر الرقمي تمثل «ثروة جديدة» تسعى الشركات والحكومات إلى جمعها وتحليلها واستغلالها. ومع دخول تقنيات الذكاء الاصطناعي في مجال تحليل البيانات، تصاعدت المخاوف بشأن تراجع خصوصية الأفراد وتحولهم إلى أهداف دائمة للرصد والمراقبة. ولم تعد القضية تقتصر على سرية البيانات فحسب، بل تجاوزت ذلك إلى تحديد سلوك الأفراد، والتنبؤ بقراراتهم، والتأثير على خياراتهم، مما يهدد استقلاليتهم الفردية ويطرح تساؤلات جوهرية حول مدى احترام الكرامة الإنسانية في ظل هذا الواقع الجديد.

لذا تنبع أهمية هذا البحث من الطابع المعاصر والعالمي لقضية الخصوصية الرقمية، وارتباطها الوثيق بحقوق الإنسان الّتي تُعدّ من الركائز الأساسية في القانون الدولي. ففي ظل تزايد الانتهاكات الرقمية، وغياب آليات رقابة فعّالة في بعض الدول، بات من الضروري إعادة النظر في الأطر القانونية والتنظيمية الكفيلة بحماية الأفراد من التعدي على خصوصياتهم، سواء من قبل الجهات الحكومية أو الشركات التكنولوجية العملاقة.

كما أن التركيز على العلاقة بين الذكاء الاصطناعي والحق في الخصوصية يتيح فرصة لفهم أعمق للتحديات المستقبلية التي قد تواجه المجتمعات، كما يُسلّط الضوء على ضرورة تطوير تشريعات مواكبة تضمن عدم استخدام هذه التقنيات الحديثة بما من شأنه أن يُلحق الضّرر بالحقوق والحريات الأساسية.

يهدف هذا البحث إلى تحليل الحق في الخصوصية الرقمية في ظل التطورات التكنولوجية الحديثة، لا سيما استخدام تقنيات الذكاء الاصطناعي والمراقبة الجماعية، ومدى انسجام هذه الممارسات مع المبادئ الأساسية لحقوق الإنسان كما نصت عليها المواثيق الدولية. ويمكن صياغة الإشكالية الرئيسة للبحث على النحو الآتي:

إلى أي مدى يُمكن اعتبار الممارسات المعاصرة في جمع البيانات وتحليلها باستخدام الذكاء الاصطناعي انتهاكًا للحق في الخصوصية كما نصّت عليه القوانين والاتفاقيات الدولية؟ وما هي آليات الحماية القانونية الممكنة لمواجهة هذه التحديات؟ ولا سيما أن بعض ممارسات جمع البيانات والتحليل الآلي باستخدام الذكاء الاصطناعي تُعدُّ انتهاكًا صريحًا للحق في الخصوصية، كذلك فإن القوانين الدولية الحالية لا تواكب بالشكل الكافي التطورات التكنولوجية المتعلقة بالخصوصية الرقمية، كما أن هناك تفاوت كبير بين الدول في احترام وتطبيق معايير الخصوصية الرقمية، مما يؤثر على فعالية الحماية العالمية.

ولهذا كان هذا البحث متوجها نحو توضيح مفهوم الحق في الخصوصية الرقمية ضمن السياقين القانوني والحقوقي، وتحليل الأطر القانونية الدولية التي تنظّم هذا الحق، ودراسة الانتهاكات المعاصرة للخصوصية الرقمية، وبيان التحديات الناتجة عن استخدام الذكاء الاصطناعي، وتقديم مقترحات وتوصيات لتعزيز الحماية القانونية للخصوصية الرقمية.

الفصل الأول: الإطار النظري للخصوصية كحق من حقوق الإنسان

يُعدّ الحق في الخصوصية من أقدم الحقوق الطبيعية التي تنبع من الكرامة الإنسانية، وقد تطور مفهومه مع تطور النظم الاجتماعية والسياسية والقانونية، حتى أصبح اليوم أحد الحقوق الأساسية المعترف بها عالميًا. في العصر الحديث، اكتسب هذا الحق أبعادًا جديدة بفعل التحول الرقمي، فلم يعد مقتصرًا على الحياة الخاصة التقليدية، بل أصبح يشمل حماية البيانات الشخصية، الاتصالات، والهوية الرقمية للأفراد[1].

في هذا الفصل، سيتم استعراض الجوانب النظرية لمفهوم الخصوصية كحق من حقوق الإنسان، وتطوره عبر مراحل القانون الدولي، مع بيان موقعه في الاتفاقيات والمعاهدات الدولية، إضافة إلى تحليل مكوناته وأنواعه المختلفة.

[1] صندوق الحرّيّة الرقميّة، (لا ت)، المادّة 12: الحقّ في الخصوصيّة.
Digital Freedom Fund, (n.d.), Article 12: The right to privacy.
https://digitalfreedomfund.org/digital-rights-are-human-rights/article-12-the-right-to-privacy/

▪ أولًا: التعريف والنشأة

1- التعريف اللغوي والاصطلاحي

لُغويًّا، تعني الخصوصية الانفراد بالأمر، أي المساحة التي يحتفظ بها الإنسان لنفسه، ولا يُريد للآخرين الاطلاع عليها، أما اصطلاحًا، عرّفها فقهاء القانون بأنّها: «الحق في أن يترك الإنسان وشأنه، وأن تكون له مساحة من الحياة غير مرئية أو متاحة للآخرين دون رضاه»[1].

ويأخذ هذا المفهوم أوجهًا عدّة، منها:

- الخصوصية الجسدية: حرمة الجسد والحماية من التفتيش غير المبرر.
- الخصوصية المعلوماتية: حماية البيانات والمعلومات الشخصية من الاستخدام غير المشروع.
- الخصوصية الاتصالية: حماية الاتصالات الهاتفية والمراسلات البريدية والإلكترونية.
- الخصوصية الفكرية: احترام الرأي والمعتقد.

2- نشأة وتطور الحق في الخصوصية

رغم أن الخصوصية لم تُصغ كحق قانوني صريح إلا حديثًا، إلا أن جذورها ضاربة في عمق الفلسفات القديمة وقد تطور هذا الحقّ في العصر الحديث عبر مراحل مُتعدّدة منها:

المرحلة الفلسفية والأخلاقية: تناولها فلاسفة مثل جون لوك وجون ستيوارت ميل، حيث دعوا إلى حماية الحريات الفردية.

المرحلة القانونية الوطنية: بدأت مع ظهور مقالات قانونية مؤثرة، أبرزها مقال «الحق في الخصوصية (The Right to Privacy)» للكاتبين صامويل وارين ولويس براندیز عام 1890[2].

المرحلة القانونية الدولية: بعد الحرب العالمية الثانية، ومع تأسيس الأمم المتحدة، أُدرج الحق في الخصوصية ضمن النصوص الدولية الملزمة.

---

[1] صندوق الحرّيّة الرقميّة، (لا ت)، المادّة 12: الحقّ في الخصوصيّة.
Digital Freedom Fund, (n.d.), Article 12: The right to privacy.
https://digitalfreedomfund.org/digital-rights-are-human-rights/article-12-the-right-to-privacy/

[2] McCraw, Thomas K, Prophets of Regulation, Harvard University Press, 1984.

3- الخصوصية في المواثيق الدولية لحقوق الإنسان

يُعتبر القانون الدولي لحقوق الإنسان المصدر الأساسي لحماية الخصوصية على المستوى العالمي، ومن أهمّ هذه الوثائق:

- **الإعلان العالمي لحقوق الإنسان 1948/12/10:** ورد في المادة 12: «لا يجوز تعريض أحد لتدخل تعسفي في حياته الخاصة أو أسرته أو مسكنه أو مراسلاته، ولا لحملات تمس شرفه وسمعته. ولكل شخص الحق في حماية القانون من مثل هذا التدخل أو تلك الحملات»[1]. يُعد هذا النص حجر الأساس في الاعتراف الدولي بالحق في الخصوصية، ورغم أنه ليس ملزمًا قانونيًا، إلا أن مكانته الأدبية والسياسية تبقى كبيرة.
- **العهد الدولي الخاص بالحقوق المدنية والسياسية 1966:** جاء في المادة 17:«لا يجوز تعريض أي شخص لتدخل تعسفي أو غير قانوني في خصوصياته أو أسرته أو بيته أو مراسلاته، ولا لأي حملات غير قانونية تمس شرفه أو سمعته من حق كل شخص أن يحميه القانون من مثل هذا التدخل أو تلك الحملات»[2]. يُعدّ هذا النص ملزمًا للدول الأطراف، مما يوفّر حماية قانونية أقوى للحق في الخصوصية، ويحمّل الدول مسؤولية منع انتهاك هذا الحق، سواء من قبل السلطات العامة أو الجهات الخاصة.
- **اتفاقيات إقليمية أخرى:**

- الاتفاقية الأوروبية لحقوق الإنسان (المادة 8): نصت على احترام الحياة الخاصة والعائلية[3].

---

[1] وثيقة الإعلان العالمي لحقوق الإنسان، الصّادر في 10/ك1948/1، منشورات الأمم المتحدة.
United Nations. (10/Dec/1948). Universal Declaration of Human Rights. https://www.un.org/en/about-us/universal-declaration-of-human-rights

[2] العهد الدّولي الخاصّ بالحقوق المدنيّة والسّياسيّة، الصّادر في 16/ك1966/1، منشورات الأمم المتحدة.
United Nations. (16/Dec/1966). International Covenant on Civil and Political Rights. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

[3] الاتفاقية الأوروبية لحقوق الإنسان، الصّادرة في 4 تشرين الثاني 1950، ودخلت حيّز التنفيذ في 3 أيلول 1953.
ECHR European Convention on Human Rights, 1950, applied on 3 Sept 1953. https://ar.wikipedia.org/wiki/الاتفاقية_الأوروبية_لحقوق_الإنسان

- الميثاق الإفريقي لحقوق الإنسان والشعوب[1]
- الاتفاقية الأمريكية لحقوق الإنسان[2]

كل هذه المواثيق تؤكد على عالمية الحق في الخصوصية بوصفه جزءًا لا يتجزأ من كرامة الإنسان.

4- مكونات الحق في الخصوصية

من خلال تحليل النصوص الدولية، يمكن تمييز المكونات التالية للحق في الخصوصية:

المكون	الشرح
الحياة الخاصة	حماية الأنشطة الشخصية من التدخل أو التطفل
الحياة الأسرية	احترام العلاقة داخل الأسرة وعدم التدخل في شؤونها
حرمة المسكن	منع دخول المنزل أو تفتيشه إلا وفق القانون
سرية المراسلات	حماية الرسائل والاتصالات أياً كانت وسائطها
البيانات الشخصية	تنظيم جمع ومعالجة البيانات وفق مبادئ الشفافية والرضا الحر
الحماية من التشهير	منع المساس بسمعة الأفراد وشرفهم دون مبرر قانوني

5- الحدود المشروعة للحق في الخصوصية

إن الحق في الخصوصية ليس مطلقًا، بل يجوز تقييده بشروط محددة وفقًا للمادة 17 من العهد الدولي[3]، وبموجب مبدأ التناسب، وذلك في الحالات التالية: حماية الأمن القومي –

---

[1] الميثاق الإفريقي لحقوق الإنسان والشّعوب، الصادر في 1981/06/27، ودخل حيّز التّنفيذ في 1986/10/21.
ACHPR African Charter on Human and Peoples' Rights, 1981, applied on 21 Oct 1986.
https://ar.wikipedia.org/wiki/الميثاق_الإفريقي_لحقوق_الإنسان_والشعوب

[2] الاتفاقية الأمريكية لحقوق الإنسان، دخلت حيّز التّنفيذ في 1978/07/18.
ACHR American Convention on Human Rights, applied on 18 July 1978.
https://ar.wikipedia.org/wiki/الاتفاقية_الأمريكية_لحقوق_الإنسان

[3] العهد الدّولي الخاصّ بالحقوق المدنيّة والسّياسيّة، الصّادر في 16/ك1/1966، منشورات الأمم المتحدة.
United Nations. (16/Dec/1966). International Covenant on Civil and Political Rights.
https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

المحافظة على النظام العام والصحة العامة – ضمان حقوق وحريات الآخرين. ولكن يجب أن تكون هذه القيود: منصوصًا عليها في القانون – ضرورية لتحقيق هدف مشروع – متناسبة مع حجم الخطر أو التهديد.

لكن مع التطور الرقمي، انتقل مفهوم الخصوصية من إطاره التقليدي إلى الفضاء الرقمي، فبرزت الحاجة إلى إعادة تنظيم هذا الحق ضمن ما يُعرف بـ «الخصوصية الرقمية». والّتي تشير إلى: «الحق في السيطرة على المعلومات الرقمية المتعلقة بالفرد، وتحديد من يملك حق الوصول إليها، وكيفية استخدامها»[1]. يفرض هذا التطور إعادة قراءة المواثيق الدولية في ضوء التحديات التقنية الحديثة، مثل الذكاء الاصطناعي، التحليل التنبؤي، والتتبع عبر الإنترنت.

▪ ثانياً: الخصوصية في العصر الرقمي

غيّرت التكنولوجيا الرقمية وجه العالم، إذ أصبحت حياتنا اليومية مرتبطة ارتباطًا وثيقًا بأجهزة الحاسوب، والهواتف الذكية، وشبكات الإنترنت، مما أتاح إمكانية غير مسبوقة للوصول إلى المعلومات وتبادلها. غير أن هذا التقدّم التقني ترافق مع تصاعد مقلق في عمليات جمع البيانات، وتزايد في تعقيد أساليب المراقبة، الأمر الذي حوّل الخصوصية من حقٍ بديهي إلى مسألة جدلية، تستوجب إعادة نظر جذرية في المفاهيم القانونية والحقوقية المرتبطة بها.

1- ملامح الخصوصية في العصر الرقمي

لم تعد الخصوصية تقتصر على الحماية من التدخّل المادي، بل باتت تشمل أيضًا المجالَين الافتراضي والرقمي، ما يعني أن أيّ تفاعل رقمي قد يكون عرضة للتتبّع، والتسجيل، والاستغلال. ويُلاحظ أن الخصوصية الرقمية تتأثر بثلاثة عناصر رئيسية[2]:

---

[1] الاتّحاد الأميركي للحرّيّات المدنيّة، 2015/03/25، الحقّ الإنساني في الخصوصيّة في العصر الرّقمي.
American Civil Liberties Union. (25/03/2015). The human right to privacy in the digital age. https://www.aclu.org/documents/human-right-privacy-digital-age

[2] الاتّحاد الأميركي للحرّيّات المدنيّة، 2015/03/25، الحقّ الإنساني في الخصوصيّة في العصر الرّقمي.
American Civil Liberties Union. (25/03/2015). The human right to privacy in the digital age. https://www.aclu.org/documents/human-right-privacy-digital-age

- **الأجهزة الذكية والتطبيقات:** الهواتف المحمولة، الساعات الذكية، تطبيقات التواصل الاجتماعي، ومحركات البحث، جميعها تُنتج وتجمع معلومات حساسة عن المستخدمين مثل الموقع الجغرافي، وعادات التصفح، والاهتمامات الشخصية.
- **تحليل البيانات الضخمة:** تُتيح تقنيات الذكاء الاصطناعي تحليل كميات هائلة من البيانات بسرعة ودقّة، مما يفتح المجال أمام التنبّؤ بسلوك الأفراد، بل وحتى التأثير في قراراتهم، وهو ما يُشكّل تهديدًا لحرية الإرادة الشخصية.
- **ضعف الوعي الرقمي:** لا يزال كثير من المستخدمين يفتقرون إلى الوعي الكافي بكيفية استخدام بياناتهم، أو بالمخاطر المرتبطة بالموافقة التلقائية على شروط الاستخدام، مما يجعلهم أكثر عرضة للاستغلال.

2- وسائل المراقبة الرقمية الحديثة

لقد تطورت أدوات المراقبة لتشمل تقنيات متقدمة يصعب اكتشافها أو تفاديها، ومن أبرزها:

الوسيلة	الشرح
كاميرات المراقبة الذكية	مزوّدة بتقنية التعرف على الوجوه وربط الأشخاص بقواعد بيانات ضخمة
برمجيات التجسس	مثل برنامج Pegasus الذي استُخدم لاختراق هواتف نشطاء وصحفيين وسياسيين
تتبع المواقع	عبر تطبيقات الهواتف وخدمات GPS
تحليل البيانات السلوكية	استخدام الذكاء الاصطناعي للتعرف على الأنماط السلوكية وتوقع التصرفات

هذه التقنيات تُستخدم أحيانًا لأغراض أمنية أو تجارية، لكنها قد تُوظف كذلك لأهداف قمعية أو سياسية، مما يثير تساؤلات قانونية وأخلاقية جدّية. لذا فإن الفضاء الرقمي قد يفتقر إلى الضوابط التي تضمن احترام الخصوصية، خاصة في ظل غموض السياسات المتعلقة بجمع البيانات، وتعدد الجهات الفاعلة فيه (الدول، الشركات، المخترقين...). وغالبًا ما يتعامل

المستخدمون مع هذه المنظومة وهم في موقع الطرف الأضعف، مما يُحتّم تدخلًا قانونيًا فعّالًا يحمي هذا الحق من التآكل[1].

وهكذا يتّضح من العرض السابق أن الخصوصية في العصر الرقمي باتت أكثر هشاشة من أيّ وقت مضى، وأن حماية هذا الحق تتطلّب فهمًا جديدًا يتجاوز الإطار التقليدي. فالتكنولوجيا التي جلبت الكثير من المنافع، قد تتحوّل بسهولة إلى أدوات للرقابة والقمع إذا تُركت دون ضوابط قانونية وأخلاقية صارمة.

▪ ثالثاً: انتهاكات الخصوصية الرقمية في السياق العالمي

على الرغم من وجود نصوص قانونية دولية تُؤكّد حق الأفراد في الخصوصية، فإن الواقع الرقمي يكشف عن ممارسات متكرّرة تنتهك هذا الحق بشكل صارخ، سواء من قِبل الحكومات، أو الشركات، أو جهات غير رسمية. في هذا الفصل، سنعرض نماذج واقعية لهذه الانتهاكات، ونُحلّل مدى توافقها مع مبادئ القانون الدولي لحقوق الإنسان، مع إبراز التحديات القانونية والأخلاقية الناتجة عنها.

1- انتهاكات الخصوصية من قبل الدول

من أبرز صور الانتهاك المعاصر لخصوصية الأفراد، لجوء بعض الدول إلى أنظمة مراقبة شاملة تفتقر إلى الرقابة القضائية، وذلك تحت ذريعة الحفاظ على الأمن القومي. وتُعد برامج مثل PRISM وXKeyscore، التي كُشف عنها في تسريبات إدوارد سنودن عام 2013، مثالًا صارخًا على ذلك. فقد استعانت هذه البرامج ببيانات وفّرتها شركات كبرى مثل Google وFacebook وMicrosoft، لجمع معلومات عن ملايين الأفراد حول العالم، دون إذن مسبق أو مبرر قانوني واضح.

وقد تستخدم بعض الأنظمة سلطاتها الرقمية لرصد النشطاء السياسيين، والصحفيين، والمعارضين، وملاحقتهم. ومن أبرز الأمثلة على ذلك: قضية برنامج **Pegasus**، الذي طوّرته

---

[1] مراقبة حقوق الإنسان، 2014/12/23، حقوق الإنسان في العصر الرّقمي.
Human Rights Watch. (2014, December 23). Human rights in the digital age. https://www.hrw.org/news/2014/12/23/human-rights-digital-age

شركة NSO الإسرائيلية، والذي استُخدم لاختراق هواتف صحفيين ومدافعين عن حقوق الإنسان في عدة دول، من بينها السعودية، والإمارات، والمكسيك، وفي الصين مثلًا، تُستخدم تقنيات التعرّف على الوجوه بشكل مفرط، حيث تطبّق الحكومة نظامًا متقدّمًا للرقابة الرقمية يشمل التعرّف على الوجوه وتحليل بيانات المواطنين ضمن ما يُعرف بـ «نظام النقاط الاجتماعية»، وهو ما يعد تدخلاً صارخًا في الحياة الخاصة[1]. كما أصبحت كاميرات الشوارع المزودة بالذكاء الاصطناعي أداة فعّالة لتعقّب الأفراد، ولا سيّما في المدن الذكية. وفي ظل غياب إطار قانوني صارم، تتحوّل هذه التقنيات إلى تهديد مباشر لحرية الحركة والخصوصية الفردية.

2- الانتهاكات من قبل الشركات الخاصة

تلجأ العديد من شركات التكنولوجيا إلى اعتماد سياسات خصوصية طويلة وغامضة، تُجبر المستخدمين على الموافقة عليها دون فهم حقيقي لمحتواها. كما تستخدم هذه الشركات ما يُعرف بـ«ملفات التتبع» (Cookies) لجمع معلومات دقيقة حول السلوك الرقمي للمستخدمين.

ولقد تعددت تسريبات أو إساءة استخدام البيانات، منها فضيحة كامبريدج أناليتيكا (2018)، حيث تم جمع بيانات أكثر من 87 مليون مستخدم لفيسبوك دون علمهم، وقد استخدمت هذه البيانات لأغراض دعائية وسياسية، لا سيما خلال الانتخابات الأمريكية[2]. وكذلك تسريبات **LinkedIn -Yahoo – Equifax**: كشفت هذه التسريبات عن إخفاق واضح في حماية بيانات مئات الملايين من المستخدمين. ومنها بيع البيانات لشركات الإعلانات وكثير من التطبيقات المجانية تُموَّل عن طريق بيع معلومات المستخدمين لشركات الإعلان الرقمي، مما يُحوّل بيانات الأفراد إلى سلعة تجارية دون علمهم أو موافقتهم الحقيقية.

3- انتهاكات الخصوصية في الأزمات والطوارئ

في فترات الطوارئ، تتساهل الدول أحيانًا في تطبيق القيود المتعلقة بالمراقبة الرقمية. فعلى سبيل المثال: خلال جائحة كوفيد-19 استخدمت بعض الدول تطبيقات لتتبع مخالطي

---

(1) مؤسسة التخوم الإلكترونية EFF، (لا ت)، المراقبة وحقوق الإنسان.
Electronic Frontier Foundation EFF. (n.d.). Surveillance and human rights. https://www.eff.org/issues/surveillance-human-rights

(2) https://ar.wikipedia.org/wiki/فضيحة_بيانات_فيسبوك-كامبريدج_أناليتيكا, 2018.

المصابين، لكن دون وجود ضمانات واضحة بشأن كيفية جمع البيانات أو المدة الزمنية للاحتفاظ بها. وقد واجهت هذه الإجراءات انتقادات من منظمات حقوقية عدة، لأنها نُفّذت دون وجود أطر قانونية واضحة توازن بين حماية الصحة العامة والحفاظ على الحق في الخصوصية.

4- مدى توافق هذه الانتهاكات مع القانون الدولي

تُعد جميع الممارسات السابقة خرقًا مباشرًا للمادتين 12 من الإعلان العالمي لحقوق الإنسان و17 من العهد الدولي للحقوق المدنية والسياسية[1]، إذ أنه: لم يتم إشعار الأفراد أو الحصول على موافقتهم، ولم تكن هناك رقابة قضائية أو شفافية، ولقد تجاوزت التدخلات الحدود المسموح بها قانونيًا، حتى في حالات الطوارئ. كما أكدت لجنة حقوق الإنسان التابعة للأمم المتحدة في تعليقها العام رقم 16 أن: «أي تدخل في الخصوصية يجب أن يكون قانونيًا وضروريًا ومتناسبًا»[2]. وبالتالي فإن جمع البيانات على نطاق واسع، دون وجود مبرر محدد أو إشراف مستقل، يمثل خرقًا لهذه المبادئ.

5- مواقف المنظمات الدولية والحقوقية

نشرت منظمة العفو الدولية وهيومن رايتس وتش تقارير متعددة تدين الانتهاكات الرقمية، لا سيما تلك المرتبطة ببرمجيات التجسس[3]. وأكدتا في تقاريرهما أن المراقبة الجماعية تُضر

---

[1] – وثيقة الإعلان العالمي لحقوق الإنسان، الصّادر في 10/ك1/1948، منشورات الأمم المتحدة.

United Nations. (10/Dec/1948). Universal Declaration of Human Rights. https://www.un.org/en/about-us/universal-declaration-of-human-rights

– العهد الدّولي الخاصّ بالحقوق المدنيّة والسّياسيّة، الصّادر في 16/ك1/1966، منشورات الأمم المتحدة.

United Nations. (16/Dec/1966). International Covenant on Civil and Political Rights. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

[2] مراقبة حقوق الإنسان، (2023)، التقرير العالمي 2023: أحداث العام 2022.

Human Rights Watch. (2023). World report 2023: Events of 2022. https://www.hrw.org/world-report/2023

[3] منظمة العفو الدوليّة، 18/تموز/2021، نطاق المراقبة السيبرانية السرية "أزمة عالمية ابتليت بها حقوق الإنسان".

Amnesty International. (2021, July 18). Scale of secretive cyber surveillance “an international human rights crisis”. https://www.amnesty.org/en/latest/press-release/2021/07/pegasus-project-spyware-digital-surveillance-nso/

بثقة المواطنين في الحكومات، وتُقوّض أسس الديمقراطية. فلقد أثبتت الوقائع أن الحق في الخصوصية يواجه تحديات جسيمة في العصر الرقمي، وأن الانتهاكات تنبع من مصادر متعددة: حكومية، وتجارية، وحتى عبر الأزمات العالمية. وبينما يتطور الواقع التقني بوتيرة سريعة، لا يزال القانون الدولي يعاني من بطء في التكيّف، مما يستدعي إجراء إصلاحات قانونية، وبناء منظومة عالمية تُلزم الفاعلين الرقميين باحترام كرامة الإنسان وحقّه في الخصوصية.

الفصل الثاني: المواقف والتشريعات الدولية لحماية الخصوصية الرقمية

تزايدت المخاوف في السنوات الأخيرة بشأن انتهاك الخصوصية الرقمية، بالتزامن مع التوسع الكبير في استخدام التقنيات الحديثة مثل الذكاء الاصطناعي، والبيانات الضخمة، وبرامج المراقبة. وقد أثارت هذه المخاوف ردود فعل قوية من المجتمع الدولي، حيث سعت الدول والمنظمات الدولية إلى سن تشريعات جديدة وتنفيذ سياسات تهدف إلى حماية الحقوق الرقمية للأفراد. في هذا الفصل، سنستعرض الردود الدولية على هذه الانتهاكات، مع التركيز على أبرز التشريعات الحديثة التي تم تطبيقها أو اقتراحها في سبيل حماية الخصوصية الرقمية.

▪ أولاً: ردود الفعل من المنظمات الدولية

يُعدّ الاتحاد الأوروبي من أبرز الجهات الفاعلة التي استجابت بسرعة لتحديات الخصوصية الرقمية، إذ أقرّ في عام 2018 اللائحة العامة لحماية البيانات **(GDPR)**، والتي تُعدّ من أكثر التشريعات شمولًا وتنظيمًا على مستوى العالم في مجال حماية البيانات الشخصية [1]. وتهدف هذه اللائحة إلى حماية حقوق الأفراد في عصر البيانات الضخمة، من خلال توفير إطار قانوني واضح يُحدّد كيفية جمع البيانات، ومعالجتها، وتخزينها[2].

---

[1] الاتّحاد الأوروبي، اللائحة العامّة لحماية البيانات، الصادرة بتاريخ 2016/04/14، ودخلت حيّز التّنفيذ في 2018/05/25.

European Union. (2016). General Data Protection Regulation (GDPR), applied on 25/05/2018. https://gdpr.eu/

[2] Kuner, Christopher. European Data Protection Law: Corporate Compliance and Regulation, Oxford University Press, 2020.

وأما أبرز معالم ال **GDPR**:

- الحق في النسيان: يحق للأفراد طلب حذف بياناتهم الشخصية من السجلات الرقمية.
- الشفافية: تلتزم الشركات والمؤسسات بالكشف عن كيفية جمع واستخدام بيانات الأفراد.
- الموافقة المسبقة: يجب على المؤسسات الحصول على موافقة واضحة وموافقة المستهلك قبل جمع البيانات.
- العقوبات: يمكن فرض غرامات تصل إلى 4% من الإيرادات السنوية للشركات المخالفة[1].

يشكّل ال **GDPR** خطوة كبيرة نحو حماية الخصوصية الرقمية لأنها تُحدّد بوضوح كيفية التعامل مع البيانات الشخصية، وتمنح الأفراد مزيدًا من الحقوق في التحكم ببياناتهم. ومع ذلك، تُواجه اللائحة تحديات في التطبيق، خصوصًا في الدول التي لا تنتمي إلى الاتحاد الأوروبي. ولهذا قضت محكمة العدل الأوروبية في قضية Schrems II عام 2020 ببطلان اتفاقية نقل البيانات بين الاتحاد الأوروبي والولايات المتحدة، بسبب عدم كفاية مستوى حماية الخصوصية في الولايات المتحدة الأمريكية[2].

كذلك فإن المقرّرة الخاصة للأمم المتحدة في تقريرها العائد للعام (2019) قد بيّنت بأن الأمم المتحدة أولت اهتمامًا خاصًا بالانتهاكات الرقمية في السنوات الأخيرة، مؤكدة أن الخصوصية تُعدّ حقًا أساسيًا يجب حمايته في العصر الرقمي. وفي تقريرها الصادر عام 2019، أطلقت المقرّرة الخاصة للأمم المتحدة دعوات قوية إلى تطوير إطار قانوني عالمي يُنظّم ممارسات جمع البيانات والمراقبة[3]. ومن أبرز التّوصيات في تقرير المقرّرة الخاصة للأمم المتحدة (2019):

---

[1] الاتّحاد الأوروبي، اللائحة العامّة لحماية البيانات، الصادرة بتاريخ 2016/04/14، ودخلت حيّز التّنفيذ في 2018/05/25.

European Union. (2016). General Data Protection Regulation (GDPR), applied on 25/05/2018. https://gdpr.eu/

[2] البرلمان الأوروبي. (2020/09/15). حكم محكمة العدل الأوروبية في قضية Schrems II.

European Parliament. (15/09/2020). The CJEU judgment in the Schrems II case. https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2020)652073

[3] مؤسسة التخوم الإلكترونية EFF، 2019، المراقبة وحقوق الإنسان.

Electronic Frontier Foundation EFF. (2019). Surveillance and human rights. https://www.eff.org/issues/surveillance-human-rights

- الدعوة إلى ضمانات قانونية قوية: أكّد التقرير على ضرورة وجود قوانين، تمنع المراقبة الجماعيّة غير المشروعة.
- تشجيع الدول على الانضمام الى الاتفاقات الدولية: دعا التقرير الدول إلى التوقيع على الاتفاقيات والمعاهدات الدولية التي تُعنى بحماية البيانات الشخصية على الصعيد الدولي.
- التأكيد على تأثير تقنيات المراقبة: حذّر التقرير من التأثيرات السلبية الواسعة لتقنيات المراقبة على حرية التعبير، والحقوق المدنية في العديد من البلدان.

▪ ثانياً: حماية البيانات في التشريعات الداخلية

أصدرت العديد من الدول قوانين ترمي إلى حماية البيانات، منها: قانون حماية البيانات في الولايات المتحدة الأمريكية، إذ على الرغم من وجود بعض القوانين الفيدرالية التي تُعنى بحماية الخصوصية في الولايات المتحدة، مثل قانون الخصوصية الأمريكي **(Privacy Act)** الذي يشمل بعض جوانب جمع البيانات، إلا أن الولايات المتحدة لا تزال تفتقر إلى تشريع شامل لحماية البيانات الشخصية كما هو الحال في الاتحاد الأوروبي[1]. ومع ذلك، ظهرت بعض التشريعات الحديثة مثل: قانون حماية خصوصية المستهلك في كاليفورنيا **(CCPA)** وهو قانون خاص بولاية كاليفورنيا يهدف إلى منح الأفراد في الولاية مزيدًا من التحكم في بياناتهم الشخصية، من خلال حقوق محددة مثل: حق الوصول إلى البيانات، حق الحذف، وحق الاعتراض على بيع البيانات الشخصية، وقانون حماية خصوصية الأطفال على الإنترنت **(COPPA)** الذي يحظر جمع البيانات الشخصية للأطفال تحت سن 13 عامًا دون موافقة الوالدين. ورغم هذه التشريعات، يبقى السؤال الأساسي في الولايات المتحدة: هل يمكن سنّ قانون شامل لحماية الخصوصية الرقمية على المستوى الفيدرالي؟

كما أقرّت الهند قانون حماية البيانات الشخصية في العام 2019 الذي يهدف إلى إنشاء إطار قانوني لحماية خصوصية المواطنين. وقد تم الإعلان عن هذا القانون بعد سنوات من الانتقادات بشأن ضعف حماية البيانات، وأبرز ما يُميّز هذا القانون هو منح الأفراد حقّ

---

[1] الاتّحاد الأميركي للحرّيّات المدنيّة، 2015/03/25، الحقّ الإنساني في الخصوصيّة في العصر الرّقمي.
American Civil Liberties Union. (25/03/2015). The human right to privacy in the digital age. https://www.aclu.org/documents/human-right-privacy-digital-age

الوصول إلى بياناتهم الشخصية، وفرض القيود على استخدام هذه البيانات من قبل الشركات[1]. في البرازيل، تم إقرار قانون حماية البيانات الشخصية **(LGPD)** في عام 2020، وهو يشبه إلى حد كبير اللائحة العامة لحماية البيانات في الاتحاد الأوروبي **(GDPR)**. يمنح هذا القانون البرازيلي المواطنين مجموعة من الحقوق، من بينها: الحق في الاطلاع على بياناتهم الشخصية، الحق في تعديلها، وحق حذفها[2].

كما تُعدّ ألمانيا من الدول التي تتمتع بأعلى معايير حماية الخصوصية الرقمية في العالم. ويتمتع المواطنون الألمان بحقوق قوية في هذا المجال، نتيجةً لتاريخ طويل من الانتهاكات التي تعرض لها الألمان خلال الحقبة النازية والفترة السوفيتية في ألمانيا الشرقية، مما عزّز الوعي العام بأهمية الخصوصية. ورغم وجود قوانين صارمة تحمي الخصوصية، تسعى بعض الشركات الألمانية إلى تطوير تقنيات تتيح مراقبة البيانات الشخصية بطريقة آمنة دون انتهاك حقوق الأفراد. ومع ذلك، لا يُسمح باستخدام هذه التقنيات لأغراض المراقبة الجماعية أو جمع البيانات بشكل غير مُبرّر[3].

وفي الصين، تعتمد الحكومة على نظام مراقبة شامل يقوم بجمع البيانات من مختلف القطاعات باستخدام تقنيات حديثة مثل الذكاء الاصطناعي والتعرف على الوجوه. يُعد هذا النظام جزءًا من استراتيجية الحكومة لتعزيز السيطرة الاجتماعية والسياسية. بحيث يُعد «نظام النقاط الاجتماعية» في الصين من أبرز الأمثلة على المراقبة الرقمية الشاملة، حيث يتم تقييم المواطنين بناءً على سلوكهم الرقمي. تُجمع البيانات من الإنترنت، ووسائل التواصل الاجتماعي، والمعاملات المالية، ليُصنّف الأفراد وفقًا لهذه المعلومات. وقد يؤدي السلوك السلبي إلى عقوبات مثل حظر السفر أو الحرمان من بعض الخدمات[4]. كما تفرض الحكومة الصينية رقابة صارمة على الإنترنت من خلال ما يُعرف بـ «جدار الحماية العظيم»، الذي

---

[1] الهند تسعى لتمرير مشروع قانون حماية البيانات الشخصية بحلول عام 2021، مجلة علوم وتكنولوجيا، 2020/10/6، الكاتب مؤنس حواس.

[2] القانون رقم 2018/13.709، القانون العام لحماية البيانات الشخصية في البرازيل.

[3] قانون حماية البيانات الفيدرالي الألماني BDSG، 2017/10/30
https://en.wikipedia.org/wiki/Bundesdatenschutzgesetz

[4] قانون حماية المعلومات الشخصية الذي نفذته الصين، "The Verge"، 2021/11/1، مجلة علوم وتكنولوجيا، سماح لبيب، 2021/8/22. http://www.youm7.com/5432985

يمنع الوصول إلى مواقع عالمية مثل فيسبوك، تويتر، وغوغل، بهدف الحد من تدفّق المعلومات الخارجية وضمان السيطرة على البيانات المتداولة محليًا.

▪ ثالثاً: التحديات التي تواجه تنفيذ التشريعات العالمية

رغم التقدم الملحوظ في التشريعات العالمية لحماية الخصوصية، لا تزال هناك تحديات كبيرة تعيق تنفيذ هذه القوانين على أرض الواقع، وأبرزها:

- **التطبيق عبر الحدود:** تزداد صعوبة تطبيق القوانين في بيئة رقمية عالمية، حيث تعمل الشركات في مناطق متعددة وبأطر قانونية مختلفة.
- **التكنولوجيا تتجاوز القانون:** في كثير من الحالات، تتطوّر التكنولوجيا بوتيرة أسرع من قدرة التشريعات على مواكبتها، لا سيما فيما يتعلق بالذكاء الاصطناعي والتعلّم الآلي. كما أن بعض التشريعات تركز على حماية أنواع محددة من البيانات الرقمية التي تُجمع على الإنترنت، مما يترك مجالًا للثغرات التشريعية في الحماية[1]. ومن المتوقّع أن تواصل الحكومات والمنظمات الدولية جهودها لتطوير تشريعات أكثر شمولًا وفعالية لحماية الخصوصية الرقمية[2]. ومن أبرز التوجهات المستقبلية: السعي نحو إقرار تشريعات موحّدة عالميًا، من خلال الدعوات المتزايدة لإبرام معاهدة دولية تُنظّم حماية الخصوصية عبر الحدود. ومع ازدياد الاعتماد على تقنيات الذكاء الاصطناعي في جمع البيانات وتحليلها، ستبقى الحاجة قائمة لتطوير قوانين تُنظّم استخدام هذه التكنولوجيا بما يضمن احترام حقوق الأفراد وعدم المساس بخصوصيتهم.

▪ رابعاً: الدراسة المقارنة بين التشريعات الأوروبية والأميركية في مجال الذكاء الاصطناعي وحماية الخصوصية

تختلف المقاربتان الأوروبية والأميركية في تنظيم الذكاء الاصطناعي اختلافًا جذريًا من حيث المنهج الفلسفي، والمبادئ القانونية، وآليات الرقابة. ففي حين يتبنى الاتحاد الأوروبي

---

(1) Zuboff, Shoshana. The Age of Surveillance Capitalism. PublicAffairs, 2019.

(2) خصوصيّة البيانات في العصر الرّقمي، 11 تموز 2024.

Singularity University. (2024, July 11). Data privacy in the digital age. https://www.su.org/resources/data-privacy-in-the-digital-age

مقاربة «وقائية قائمة على الحقوق الأساسية»، تُفضّل الولايات المتحدة مقاربة «براغماتية ليبرالية قائمة على الابتكار».

في المنظور الأوروبي تعدّ اللائحة العامة لحماية البيانات (GDPR) المرجعية الأسمى لحماية البيانات في أوروبا. وكذلك فإن قانون الذكاء الاصطناعي الأوروبي – (AI Act 2024): أول قانون شامل في العالم ينظّم الذكاء الاصطناعي وفقًا لمستوى المخاطر وهو يتضمن المبادئ الأساسية: الاحتراز، الشفافية، حقوق الأفراد، المساءلة. كما يتضمّن تصنيف المخاطر ضمن فئات: ممنوعة كليًا، عالية الخطورة، محدودة الخطورة، منخفضة الخطورة.

أما في المنظور الأميركي فلا يوجد قانون فدرالي شامل إنما يوجد قوانين قطاعية مثل CCPA, HIPAA, FCRA. أما المبادئ الأساسية لهذه القوانين فهي: التركيز على الابتكار، التوجيه الذاتي، غياب مبدأ الحق في التفسير. وقد تمّ إقرار إعلان حقوق الذكاء الاصطناعي 2022 (توجيهي).

وفيما يلي جدول المقارنة التفصيلية بين أوروبا وأميركا:

المعيار	الاتحاد الأوروبي	الولايات المتحدة
الطبيعة القانونية	إلزامية وموحّدة (GDPR + AI Act)	غير موحّدة، وقطاعية
الحق في التفسير	مكفول	غير منصوص عليه
تصنيف المخاطر	منصوص عليه	غير موجود
آليات الرقابة	هيئات مركزية	هيئات متفرقة
نهج التنظيم	حقوقي وقائي	ابتكاري مرن
الشفافية	إلزامية	اختيارية
أمن البيانات	شامل ومتعدد	محدود ومركّز على الأمن السيبراني
تأثير القطاع الخاص	محدود	واسع

وهكذا يتضح من الاستجابات الدولية والتشريعات الحديثة أن هناك جهودًا حثيثة تُبذل لحماية الخصوصية الرقمية في ظل التحديات الكبيرة التي تفرضها التقنيات الحديثة. ومع ذلك، لا تزال هناك عقبات قانونية، اجتماعية وتقنية يجب التغلب عليها لضمان التّطبيق الفعّال لهذه القوانين في حماية الحقوق الرقمية للأفراد. ويُحتّم المستقبل اعتماد تحديثات مستمرة، إلى جانب تعزيز التعاون العالمي بين الحكومات، والشركات، والمجتمع المدني، لضمان أن تظل الخصوصية الرقمية حقًا أساسيًا لا يمكن انتهاكه.

▪ خامساً: التحديات المستقبلية

تُعد حماية الخصوصية الرقمية في عصر التكنولوجيا الحديثة من أكبر التحديات التي يواجهها المجتمع الدولي. ومع التطور السريع للتقنيات، مثل الذكاء الاصطناعي، والبيانات الضخمة، وإنترنت الأشياء، تزداد الحاجة إلى ضمان قدرة الأفراد على الحفاظ على حقوقهم في الخصوصية ضمن عالم مترابط رقميًا.

1- التحديات المرتبطة بالذكاء الاصطناعي

مع تزايد استخدام الذكاء الاصطناعي في تحليل البيانات الشخصية، يتصاعد القلق حول كيفية جمع هذه البيانات واستخدامها. إذ باتت الخوارزميات الحديثة قادرة على التنبؤ بسلوك الأفراد بدقّة، مما يؤدي إلى اختراق الخصوصية الشخصية ويُعرّض الأفراد للاستغلال[1]. كما تلجأ العديد من الدول والشركات إلى تقنيات الذكاء الاصطناعي في المراقبة الجماعية، مثل تقنيات التعرف على الوجوه وتتبع المواقع. وتشكل هذه الممارسات تهديدًا مباشرًا للحرية الشخصية، وتزيد من مخاطر استخدام هذه التقنيات في تقييد الحريات.

[1] منظّمة العفو الدّوليّة 2023، الانقسام الرقمي: التكنولوجيا، التّباين، وحقوق الإنسان.
Amnesty International. (2023). Digitally divided: Technology, inequality and human rights. https://www.amnesty.org/en/documents/pol40/7108/2023/en/

2- التحديات القانونية والتنظيمية

تُعد قوانين الخصوصية في العديد من الدول غير متوافقة أو غير متناسقة، لا سيما في ظل عالم معولم تتجاوز فيه البيانات الحدود الوطنية. ويُعقّد هذا الوضع عملية تطبيق القوانين، خصوصًا على الشركات متعددة الجنسيات التي تقوم بجمع وتخزين البيانات عبر دول متعددة.

3- تحقيق التوازن بين الأمان والخصوصية

في ظل تهديدات الهجمات السيبرانية والإرهاب، تسعى الحكومات إلى تحسين الأمان الرقمي من خلال زيادة المراقبة. لكن هذا يخلق توترًا بين الحفاظ على الأمان وحق الأفراد في الخصوصية[1]. التحدي يكمن في تحقيق توازن بين هذين العنصرين دون التضحية بأحدهما لصالح الآخر. ومع تزايد استخدام التقنيات الرقمية، تزداد أيضًا الهجمات السيبرانية، مما يؤدي إلى تسريب البيانات الشخصية. فالهجمات التي تستهدف البنى التحتية الرقمية، مثل الأنظمة المصرفية أو المؤسسات الحكومية، قد تؤدي إلى سرقة بيانات حساسة والتسبب في أضرار هائلة للأفراد والمجتمعات[2]. وفي حالات الطوارئ مثل جائحة كورونا، قد تُستخدم تقنيات جمع البيانات لاحتواء الأزمات الصحية. ومع ذلك، قد يؤدي استخدام هذه البيانات إلى التعدي على الخصوصية الشخصية للأفراد. التحدي هنا هو في كيفية استخدام هذه البيانات بطريقة تحترم الخصوصية الفردية، مع تحقيق الأهداف الصحية العامة.

4- الخصوصية في المستقبل: خصوصية الأطفال والضعفاء

تُعدّ حماية خصوصية الأطفال والضعفاء من أكبر التحديات المستقبلية. فمع تزايد استخدام الإنترنت بين الأطفال والشباب، تصبح بياناتهم عرضة للاختراق من قبل الشركات

---

[1] آرثر بايبر، 2025، تهديد المراقبة الرقمية لحقوق الإنسان، رابطة المحامين الدوليين.

Piper, A. 2025, Digital surveillance's threat to human rights. International Bar Association. https://www.ibanet.org/Article/NewDetail?ArticleUid=CEE365AB-CC04-4E2C-91F6-D5F4D353A0A0

[2] مراقبة حقوق الإنسان، 2014/12/23، حقوق الإنسان في العصر الرّقمي.

Human Rights Watch. (2014, December 23). Human rights in the digital age. https://www.hrw.org/news/2014/12/23/human-rights-digital-age

والمجرمين[1]. يحتاج النظام القانوني إلى توفير حماية خاصة لهذه الفئات لضمان عدم استغلال بياناتهم.

ولهذا سيظلّ مستقبل حماية الخصوصية الرقمية مليئًا بالتحديات. ومن الضروري تطوير تشريعات وتقنيات قادرة على مواجهة هذه التحديات، مع الحفاظ على توازن دقيق بين الأمان والخصوصية. كما يجب تعزيز التعاون الدولي وتوحيد الجهود لحماية الخصوصية في عالم دائم التغيّر.

▪ سادساً: الاستنتاجات والتوصيات

شهد العالم تطورًا تكنولوجيًا غير مسبوق في السنوات الأخيرة، مما أثر بشكل كبير على جميع جوانب حياتنا، بما في ذلك خصوصيتنا الرقمية. وفي هذا السياق، أصبح الحق في الخصوصية الرقمية جزءًا لا يتجزأ من حقوق الإنسان الأساسية التي يجب أن تحظى بالحماية[2]. لقد تناولنا في هذا البحث أهمية هذا الحق، والتحديات التي يواجهها في عصر الذكاء الاصطناعي والمراقبة الجماعية، بالإضافة إلى مقارنة بين نماذج حماية الخصوصية في دول مختلفة. وفي هذا الفصل، سنستعرض أهم الاستنتاجات التي تم التوصل إليها، إلى جانب التوصيات التي يمكن أن تسهم في تعزيز حماية الخصوصية الرقمية في المستقبل.

1- أهمية الحق في الخصوصية الرقمية: يتبيّن من خلال هذا البحث أن الحق في الخصوصية الرقمية يُعد من الحقوق الأساسية التي يجب حمايتها بشكل فعّال في العصر الرقمي. ومع تزايد استخدام التقنيات الحديثة، مثل الذكاء الاصطناعي والبيانات الضخمة، أصبح من الصعب على الأفراد الحفاظ على خصوصيتهم الشخصية في ظل المراقبة الجماعية المستمرة.

---

[1] مركز جنيف لتعزيز حقوق الإنسان والحوار العالمي، حزيران 2023، المراقبة وحقوق الإنسان: ملخص تحليلي.
Geneva Centre for Human Rights Advancement and Global Dialogue. (2023, June). Surveillance and human rights: Background paper. https://gchragd.org/wp-content/uploads/2023/06/GCHRAGD-SURVEILLANCE-AND-HUMAN-RIGHTS-background-paper.pdf

[2] شاليزا يعقوب صدّيقي، سارة فاروقي، وجيه الرحمن، لابا ذو الفقار، 2024/08/30، حقوق الإنسان في العصر الرقمي.
Siddiqui, S. Y., Farooqi, S., ur Rehman, W., & Zulfiqar, L. (2024, August 30). Human rights for the digital age. https://arxiv.org/abs/2408.17302

2- التحديات المعاصرة لحماية الخصوصية: من أبرز التحديات التي تم تحديدها، الاستخدام المتزايد للتقنيات في جمع وتحليل البيانات الشخصية، خاصةً في ظل غياب قوانين متناسقة على المستوى الدولي. علاوة على ذلك، تُعدّ التهديدات الأمنية، مثل الهجمات السيبرانية، من أكبر المخاطر التي تهدد حماية الخصوصية الرقمية[1]. كما أن التحديات القانونية والتنظيمية تتعلق بعدم توافق قوانين الخصوصية في الدول المختلفة، مما يعرقل جهود حماية البيانات الشخصية عبر الحدود.

3- الاختلافات بين الدول في حماية الخصوصية: لقد تبين من خلال الدراسة المقارنة بين الدول، أنها تتبنى نماذج متفاوتة في تعاملها مع الخصوصية الرقمية. هذا الاختلاف يعود إلى عوامل ثقافية، تاريخية، وسياسية تؤثر على كيفية تعامل كل دولة مع الخصوصية.

4- المستقبل والتحديات القادمة: ظهر الدراسة أن الخصوصية الرقمية ستظل تواجه تحديات كبيرة في المستقبل، خصوصًا في ظل التقدم السريع في الذكاء الاصطناعي. من المهم تطوير تقنيات جديدة تضمن حماية البيانات الشخصية، بالإضافة إلى تعزيز التعاون بين الدول لتوحيد المعايير المتعلقة بالخصوصية الرقمية.

أما أبرز التوصيات فتتمثّل بما يأتي:

1- تطوير تشريعات عالمية موحدة: من الضروري أن تعمل الدول على تطوير تشريعات عالمية موحدة تضمن حماية الخصوصية الرقمية. يجب أن يتم تعزيز الاتفاقيات الدولية، مثل اللائحة العامة لحماية البيانات **GDPR**، ليتم تطبيقها بشكل أكثر فعالية عبر الدول المختلفة. كما يجب توفير آليات واضحة لمعاقبة الشركات والدول التي تنتهك الخصوصية.

2- تعزيز استخدام التقنيات لحماية الخصوصية: ينبغي الاستثمار في تطوير تقنيات مثل التشفير وحماية البيانات باستخدام الذكاء الاصطناعي لمواجهة التهديدات المتزايدة. يمكن أيضًا استحداث أنظمة تتبع تستخدم الذكاء الاصطناعي لاكتشاف الانتهاكات المتعلقة بالخصوصية بشكل فوري. من الممكن أن يتم استخدام التقنيات الحديثة لحماية الأفراد بدلاً من تهديد خصوصيتهم.

---

[1] صندوق الحرّيّة الرقميّة، (لا ت)، المادّة 12: الحقّ في الخصوصيّة.
Digital Freedom Fund, (n.d.), Article 12: The right to privacy.
https://digitalfreedomfund.org/digital-rights-are-human-rights/article-12-the-right-to-privacy/

3- توعية الأفراد وتعليمهم حقوقهم الرقمية: تعدّ التوعية بحقوق الخصوصية الرقمية أمرًا بالغ الأهمية. يجب على الحكومات والمنظمات الدولية تكثيف جهود التوعية من خلال حملات إعلامية وتعليمية تشرح للأفراد كيفية حماية بياناتهم الشخصية، وما هي حقوقهم في مجال الخصوصية. يتعين أن يكون الأفراد على دراية بالأساليب التي يمكنهم اتباعها لحماية أنفسهم من تسريب البيانات أو الاستغلال.

4- تحقيق التوازن بين الأمان والخصوصية: يجب أن تتبنى الحكومات والهيئات المعنية نهجًا متوازنًا بين حماية الأفراد وحقوقهم في الخصوصية، وبين الاحتياجات الأمنية التي تفرضها الأزمات أو التهديدات السيبرانية. من المهم وضع حدود واضحة لاستخدام تقنيات المراقبة، والتأكد من أنها لا تتجاوز إطار الأمان إلى التعدي على الحقوق الشخصية.

5- حماية خصوصية الفئات الضعيفة: من الضروري أن تتضمن التشريعات المستقبلية بنودًا خاصة لحماية خصوصية الفئات الضعيفة مثل الأطفال، كبار السن، وذوي الاحتياجات الخاصة. يجب أن تحظى هذه الفئات بحماية قانونية إضافية تضمن عدم استغلال بياناتها الشخصية أو استخدامها بشكل يضر بمصالحها.

الخاتمة

في الختام، يُعد الحق في الخصوصية الرقمية من الحقوق التي يجب أن تحظى بحماية قوية وفعّالة في عصرنا الرقمي. يتطلب الحفاظ على هذا الحق التعاون بين الدول، وتفعيل التشريعات الدولية، وتطوير تقنيات متقدمة تضمن حماية بيانات الأفراد. إن تزايد الانتهاكات الرقمية وغياب الرقابة الفعالة في بعض الدول يفرضان ضرورة إعادة النظر في الأطر القانونية والتنظيمية لضمان حماية الأفراد من انتهاك خصوصياتهم. وتشمل هذه الانتهاكات جمع البيانات دون موافقة، واستخدام تقنيات المراقبة الجماعية بشكل يمسّ بالحريات الأساسية[1].

[1] مكتب الأمم المتّحدة لحقوق الإنسان، 15 أيلول 2022، برامج التجسس والمراقبة: تفاقم المخاطر التي تهدّد الخصوصية وحقوق الإنسان – تقرير للأمم المتحدة.

United Nations Human Rights Office. (2022, September 15). Spyware and surveillance: Threats to privacy and human rights growing – UN report. https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report

أضحت قضية الخصوصية الرقمية تكتسب أهمية متزايدة في العصر الحديث، حيث أصبحت من المسائل المحورية على الصعيدين المحلي والدولي. ويعود ذلك إلى التطور التكنولوجي المتسارع وانتشار تقنيات الذكاء الاصطناعي، التي أدت إلى توسع غير مسبوق في جمع البيانات الشخصية ومراقبتها. في ظل هذه التحولات، يرتبط الحق في الخصوصية الرقمية ارتباطًا وثيقًا بحقوق الإنسان، التي تُعتبر من الركائز الأساسية في القانون الدولي، وينبغي أن يُعالج على أنه مكوّن أساسي للاستقرار الاجتماعي والثقة في العهد الرقمي الحديث.

علاوة على ذلك، يتعين على الأفراد أن يكونوا على دراية تامة بكيفية حماية أنفسهم في ظل تطور التقنيات والمراقبة المستمرة. ومن خلال ما أبديناه من توصيات، يمكن أن نحقق بيئة رقمية تحترم الخصوصية وتحافظ على كرامة الأفراد في المستقبل.

المراجع

- قانون حماية المعلومات الشخصية الذي نفذته الصين، "The Verge"، 2021/11/1، مجلة علوم وتكنولوجيا، سماح لبيب، 2021/8/22، 5432985/http://www.youm7.com
- القانون رقم 2018/13.709، القانون العام لحماية البيانات الشخصية في البرازيل.
- الهند تسعى لتمرير مشروع قانون حماية البيانات الشخصية بحلول عام 2021، مجلة علوم وتكنولوجيا، 2020/10/6، الكاتب مؤنس حواس.
- الميثاق الإفريقي لحقوق الإنسان والشّعوب، الصادر في 1981/06/27، ودخل حيّز التّنفيذ في 1986/10/21.

ACHPR African Charter on Human and Peoples' Rights, 1981, applied on 21 Oct 1986. https://ar.wikipedia.org/wiki/الميثاق_الإفريقي_لحقوق_الإنسان_والشعوب

- الاتفاقية الأمريكية لحقوق الإنسان، دخلت حيّز التّنفيذ في 1978/07/18.

ACHR American Convention on Human Rights, applied on 18 July 1978. https://ar.wikipedia.org/wiki/الاتفاقية_الأمريكية_لحقوق_الإنسان

- منظمة العفو الدوليّة، 18/تموز/2021، نطاق المراقبة السيبرانية السرية "أزمة عالمية ابتليت بها حقوق الإنسان".

Amnesty International. (2021, July 18). Scale of secretive cyber surveillance "an international human rights crisis". https://www.amnesty.org/en/latest/press-release/2021/07/pegasus-project-spyware-digital-surveillance-nso/

- منظّمة العفو الدّوليّة 2023، الانقسام الرقمي: التكنولوجيا، التّباين، وحقوق الإنسان.

Amnesty International. (2023). Digitally divided: Technology, inequality and human rights. https://www.amnesty.org/en/documents/pol40/7108/2023/en/

- الاتّحاد الأميركي للحرّيّات المدنيّة، 2015/03/25، الحقّ الإنساني في الخصوصيّة في العصر الرّقمي.

American Civil Liberties Union. (25/03/2015). The human right to privacy in the digital age. https://www.aclu.org/documents/human-right-privacy-digital-age

- صندوق الحرّيّة الرقميّة، (لا ت)، المادّة 12: الحقّ في الخصوصيّة.

Digital Freedom Fund, (n.d.), Article 12: The right to privacy. https://digitalfreedomfund.org/digital-rights-are-human-rights/article-12-the-right-to-privacy/

- الاتفاقية الأوروبية لحقوق الإنسان، الصّادرة في 4 تشرين الثاني 1950، ودخلت حيّز التنفيذ في 3 أيلول 1953.

ECHR European Convention on Human Rights, 1950, applied on 3 Sept 1953. https://ar.wikipedia.org/wiki/الاتفاقية_الأوروبية_لحقوق_الإنسان

- مؤسسة التخوم الإلكترونية EFF، (لا ت)، المراقبة وحقوق الإنسان.

Electronic Frontier Foundation EFF. (n.d.). Surveillance and human rights. https://www.eff.org/issues/surveillance-human-rights

- الاتّحاد الأوروبي، اللائحة العامّة لحماية البيانات، الصادرة بتاريخ 2016/04/14، ودخلت حيّز التّنفيذ في 2018/05/25.

European Union. (2016). General Data Protection Regulation (GDPR), applied on 25/05/2018. https://gdpr.eu/

- البرلمان الأوروبي. (2020/09/15). حكم محكمة العدل الأوروبية في قضية Schrems II.

European Parliament. (15/09/2020). The CJEU judgment in the Schrems II case. https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2020)652073

- مركز جنيف لتعزيز حقوق الإنسان والحوار العالمي، حزيران 2023، المراقبة وحقوق الإنسان: ملخص تحليلي.

Geneva Centre for Human Rights Advancement and Global Dialogue. (2023, June). Surveillance and human rights: Background paper. https://gchragd.org/wp-content/uploads/2023/06/GCHRAGD-SURVEILLANCE-AND-HUMAN-RIGHTS-background-paper.pdf

- مراقبة حقوق الإنسان، 2014/12/23، حقوق الإنسان في العصر الرّقمي.

Human Rights Watch. (2014, December 23). Human rights in the digital age. https://www.hrw.org/news/2014/12/23/human-rights-digital-age

- مراقبة حقوق الإنسان، (2023)، التقرير العالمي 2023: أحداث العام 2022.

Human Rights Watch. (2023). World report 2023: Events of 2022. https://www.hrw.org/world-report/2023

- آرثر بايبر، 2025، تهديد المراقبة الرقمية لحقوق الإنسان، رابطة المحامين الدوليين.

Piper, A. 2025, Digital surveillance's threat to human rights. International Bar Association. https://www.ibanet.org/Article/NewDetail?ArticleUid=CEE365AB-CC04-4E2C-91F6-D5F4D353A0A0

- شاليزا يعقوب صدّيقي، سارة فاروقي، وجيه الرحمن، لابا ذو الفقار، 2024/08/30، حقوق الإنسان في العصر الرقمي.

Siddiqui, S. Y., Farooqi, S., ur Rehman, W., & Zulfiqar, L. (2024, August 30). Human rights for the digital age. https://arxiv.org/abs/2408.17302

- خصوصيّة البيانات في العصر الرّقمي، 11 تموز 2024.

Singularity University. (2024, July 11). Data privacy in the digital age. https://www.su.org/resources/data-privacy-in-the-digital-age

- وثيقة الإعلان العالمي لحقوق الإنسان، الصّادر في 10/ك1/1948، منشورات الأمم المتحدة.

United Nations. (10/Dec/1948). Universal Declaration of Human Rights. https://www.un.org/en/about-us/universal-declaration-of-human-rights

- العهد الدّولي الخاصّ بالحقوق المدنيّة والسّياسيّة، الصّادر في 16/ك1/1966، منشورات الأمم المتحدة.

United Nations. (16/Dec/1966). International Covenant on Civil and Political Rights. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

- مكتب الأمم المتّحدة لحقوق الإنسان، 15 أيلول 2022، برامج التجسس والمراقبة: تفاقم المخاطر التي تهدّد الخصوصية وحقوق الإنسان – تقرير للأمم المتحدة.

United Nations Human Rights Office. (2022, September 15). Spyware and surveillance: Threats to privacy and human rights growing – UN report. https://www.ohchr.org/en/press-releases/2022/09/spyware-and-surveillance-threats-privacy-and-human-rights-growing-un-report

- McCraw, Thomas K, Prophets of Regulation, Harvard University Press, 1984.
- Kuner, Christopher. European Data Protection Law: Corporate Compliance and Regulation, Oxford University Press, 2020.
- Zuboff, Shoshana. The Age of Surveillance Capitalism. PublicAffairs, 2019.
- https://wikipedia.org/wiki/