

الحق في الخصوصية الرقمية بين حماية البيانات ومتطلبات الأمن الوطني: قراءة استشرافية

Digital Privacy Rights Between Data Protection and National Security Requirements: A Forward-Looking Analysis

تاريخ القبول: 20.././..

تاريخ الإرسال: 20.././..



Khalil SOLTANI	خليل سلطاني	Abderzag SAHRAOUI	عبد الرزاق صحراوي*
مخبر الحوكمة والقانون الاقتصادي		مخبر الائتلاء مؤسسة الائتلاء1	
University of Batna1		University Center of Illizi, Algeria	
khalil.soltani@univ-batna.dz رقم الهاتف: 0661256544		sahraoui.abderzag@cuillizi.dz رقم الهاتف: 0657875212	

من جهة، ومتطلبات الأمن الوطني كضرورة اجتماعية وسيادية من جهة أخرى. تسعى هذه الدراسة إلى تقديم قراءة استشرافية لمستقبل هذه المعادلة المعقدة، من خلال تحليل التطور المتوقع للإطار التشريعي لحماية البيانات، واستكشاف حدود تدخل الدولة في جمع المعلومات ومعالجتها، وتقييم آفاق تحقيق توازن عقلائي بين الخصوصية ومتطلبات الأمن في ظل توسع الذكاء الاصطناعي، الحوسبة السحابية، والبيانات الضخمة. وتخلص الدراسة إلى ضرورة تبني مقاربة شمولية تجمع بين الإصلاح القانوني، الحلول التقنية

ملخص:

عرفت البيئة الرقمية خلال العقدین الأخيرین تحولات عميقة جعلت البيانات الرقمية محوراً أساسياً في المعاملات الفردية والمؤسسية، مما أعاد طرح مسألة الخصوصية الرقمية بوصفها أحد أبرز الحقوق المرتبطة بالكرامة الإنسانية. وفي المقابل، أدى تنامي التهديدات السيبرانية وجرائم الفضاء الرقمي إلى زيادة اعتماد الدول على آليات جمع البيانات ومعالجتها لأغراض الحماية والمحافظة على الأمن الوطني. وتثير هذه الازدواجية إشكالية مركزية تتمثل في كيفية التوفيق بين حماية الخصوصية الرقمية كحق أساسي

الكلمات المفتاحية: الخصوصية الرقمية؛ حماية البيانات؛ الأمن الوطني؛ الذكاء الاصطناعي؛ البيانات الضخمة؛ الأمن السيبراني؛ التشريعات الرقمية.

الضامنة للخصوصية، وتعزيز ثقافة الوعي الرقمي من أجل بناء نموذج مستقبلي يحقق الأمن دون التضحية بالحقوق الأساسية للمواطن الرقمي.

Abstract:

Over the past two decades, the digital environment has undergone profound transformations that have made digital data a central element of individual and institutional interactions. This evolution has brought digital privacy to the forefront as a fundamental human right. At the same time, the rise of cyber threats and digital-space crimes has increased states' reliance on data collection and processing mechanisms to safeguard national security. This duality raises a central question: how can digital privacy as a fundamental right be reconciled with national security as a social and sovereign necessity?

This paper offers a forward-looking analysis of the future balance between these two imperatives by examining the anticipated evolution

of data-protection legislation, exploring the limits of state intervention in data collection and processing, and assessing the prospects of achieving a reasonable equilibrium between privacy and security in an era shaped by artificial intelligence, cloud computing, and big data. The study concludes that an effective future model requires a comprehensive approach combining legal reform, privacy-preserving technological solutions, and enhanced digital-literacy culture to ensure national security without compromising the essential rights of the digital citizen.

Keywords:

Digital privacy; Data protection; National security; Artificial intelligence; Big data; Cybersecurity; Digital legislation.

مقدمة:

شهد العالم خلال العقود الأخيرة توسعاً غير مسبوق في استخدام الفضاء الرقمي، ما جعل البيانات الشخصية تحتل موقعاً محورياً في الحياة اليومية للأفراد وفي أداء المؤسسات العامة والخاصة على حدّ سواء. ومع هذا التحول العميق، برز الحق في الخصوصية الرقمية باعتباره أحد أهم الحقوق المرتبطة بصون الهوية الإنسانية، في وقت أصبحت فيه البيانات تُعدّ مورداً استراتيجياً توظفه الدول لتعزيز أمنها الوطني ومواجهة التهديدات السيبرانية المتنامية. هذا التداخل بين متطلبات حماية الحياة الخاصة وضرورات الأمن العام ولّد نقاشاً قانونياً متجدداً حول حدود تدخل الدولة في جمع البيانات ومعالجتها، وكيفية صياغة نماذج تشريعية وتقنية قادرة على تحقيق المعادلة الصعبة بين الحق والأمن في ظل الثورة الرقمية المتسارعة، خاصة مع صعود الذكاء الاصطناعي، الحوسبة السحابية، والبيانات الضخمة.

وفي ظل هذا المشهد المعقد، تبرز الإشكالية المركزية الآتية:

إلى أي مدى يمكن بناء نموذج مستقبلي يحقق توازنًا عقلائيًا بين حماية الخصوصية الرقمية ومتطلبات الأمن الوطني في ظل التحولات التقنية المتسارعة؟

وللإجابة على هذه الإشكالية، تقوم هذه المداخلة على خطة ثنائية المحاور؛ يتناول محورها الأول حماية الخصوصية الرقمية في سياق التحول الرقمي، بينما يركز محورها الثاني على الأمن الوطني بين ضرورات جمع البيانات واستشراف المستقبل الرقمي.

المحور الأول: حماية الخصوصية الرقمية في ظل التحول الرقمي

مع تسارع التحول الرقمي واتساع نطاق استخدام البيانات في مختلف المجالات، أصبحت الخصوصية الرقمية إحدى القضايا الأكثر إلحاحًا في النقاش القانوني المعاصر. فقد انتقلت البيانات الشخصية من مجرد معلومات فردية إلى مورد استراتيجي تتنافس عليه المؤسسات وتستند إليه الحكومات في إدارة الشؤون العامة والرقمية. هذا الواقع الجديد فرض على المشرعين إعادة النظر في الأطر القانونية التقليدية التي باتت عاجزة عن مواكبة التحديات التقنية المتنامية، كما وضع موضوع حماية الخصوصية الرقمية في قلب الاهتمامات الدستورية والحقوقية. وفي هذا السياق، يقتضي تحليل خصوصية الفرد في البيئة الرقمية دراسة التطور التشريعي والمعايير الدولية التي تشكل مرجعًا أساسيًا لتنظيم حماية البيانات، إضافة إلى الوقوف على حدود هذا الحق في ظل متطلبات المعالجة الحديثة للبيانات وما تفرضه من موازنة بين الضمانات الدستورية واعتبارات الفاعلية الرقمية.

أولاً- التطور التشريعي لحماية البيانات الشخصية والمعايير الدولية ذات الصلة

عرفت حماية البيانات الشخصية تطورًا تشريعيًا ملحوظًا خلال العقود الأخيرة، نتيجة التحول الرقمي المتسارع وتنامي دور النظم المعلوماتية في إدارة المعاملات العامة والخاصة. وقد أدركت الدول، مبكرًا، أن توسع المعالجة الآلية للبيانات يطرح مخاطر جدية تتعلق بالمساس بالحياة الخاصة وإمكانية إساءة استعمال المعلومات، مما دفعها إلى تبني قواعد قانونية جديدة تعيد ضبط العلاقة بين الفرد والجهات المعالجة.

1- البدايات الأولى لتقنين حماية البيانات الشخصية

ترجع الإرهاصات الأولى لحماية البيانات الشخصية إلى أوروبا خلال السبعينيات والثمانينيات، غير أن المؤسسة الحقيقية لهذا الحق ظهرت مع اتفاقية مجلس أوروبا رقم 108 لسنة 1981 بشأن حماية الأفراد تجاه المعالجة الآلية للبيانات ذات الطابع الشخصي⁽¹⁾. وتعتبر هذه الاتفاقية أول صك دولي ملزم في هذا المجال، وقد أرسيت مبادئ جوهرية منها: الشفافية، تحديد الغرض، جودة البيانات، والحق في الوصول والتصحيح.

2- التحول نحو منظومة حماية متقدمة: اللائحة الأوروبية GDPR

أحدث صدور اللائحة العامة لحماية البيانات الأوروبية (GDPR) سنة 2016 تحولًا نوعيًا في فلسفة حماية البيانات⁽²⁾، إذ وضعت إطارًا شاملاً ومتقدمًا يعتمد على مبادئ صارمة كالشفافية، المسؤولية، تقليل

البيانات، وحماية الخصوصية بحكم التصميم. كما رتخت اللائحة حقوقًا موسّعة للأفراد مثل: الحق في النسيان، الاعتراض على المعالجة، قابلية نقل البيانات، وحق الإخطار بوقوع اختراقات. كما فرضت اللائحة التزامات جديدة على المؤسسات، من بينها:

- أ. تعيين مسؤول لحماية البيانات (DPO) في المؤسسات التي تقوم بمعالجة واسعة.
 - ب. إنجاز تقييمات أثر حماية البيانات (DPIA) عند القيام بمعالجات عالية الخطورة.
- توسيع نطاق التطبيق ليشمل الجهات خارج الاتحاد الأوروبي التي تستهدف بيانات المواطنين.
- 3- المعايير الدولية والإقليمية الحديثة ذات الصلة
- بالإضافة إلى الإطار الأوروبي، تشكل مجموعة من الوثائق الدولية مرجعًا أساسيًا في تنظيم حماية البيانات، أهمها:

- أ. مبادئ منظمة التعاون الاقتصادي والتنمية *OECD* (تحديث 2025) بشأن حماية الخصوصية وتدفق البيانات.⁽³⁾
- ب. قرار الجمعية العامة للأمم المتحدة لسنة 2014 حول الحق في الخصوصية في العصر الرقمي.⁽⁴⁾
- ج. اتفاقية الأمم المتحدة للأمن السيبراني المعتمدة في بودابست عام 2001، التي تُعد إطارًا مكملًا لضمان حماية البيانات أثناء التحقيقات في الجرائم الإلكترونية.⁽⁵⁾ ومع أن ستين بلدًا قد صادق عليها في نفس السنة، فإنها واجهت عدة تحديات، ورأت بعض الدول أنها باتت قديمة وغير قادرة على معالجة التحديات السيبرانية الحالية، وهو ما دفع إلى اعتماد اتفاقية جديدة، وهو ما تحقق في سنة 2024.

- د. اتفاقية الأمم المتحدة لمكافحة الجرائم الإلكترونية المعتمدة بنيويورك سنة 2024، والتي تهدف إلى تحسين طرق منع الجرائم الإلكترونية ومواجهتها، وتعزيز التعاون الدولي لمكافحة الجرائم الإلكترونية، وتوفير المساعدة الفنية وبناء القدرات لا سيّما للبلدان النامية.⁽⁶⁾

4- تطور التشريعات الوطنية في الدول النامية والعربية

شهدت عدة دول عربية وإفريقية تبني تشريعات خاصة بحماية البيانات الشخصية، مع تفاوت في مستوى تطورها ودرجة استقلال الهيئات لرقابية. ويمكن الإشارة إلى بعض النماذج:

- أ. مصر: قانون رقم 151 لسنة 2020 بشأن حماية البيانات الشخصية.
- ب. الإمارات العربية المتحدة: المرسوم بقانون اتحادي رقم 45 لسنة 2021.

ج. المغرب: القانون رقم 08-09 لسنة 2009 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات.

د. تونس: القانون الأساسي عدد 63 لسنة 2004 حول حماية المعطيات الشخصية.

هـ. أما بالنسبة للجزائر، فيُعد القانون رقم 07-18 المؤرخ في 10 يونيو 2018 بشأن حماية الأشخاص الطبيعيين في معالجة البيانات ذات الطابع الشخصي الإطار التشريعي الأساسي في هذا المجال. والذي عرّف المعطيات ذات الطابع الشخصي - بأنها "كل معلومة بغض النظر عن دعائها متعلقة بشخص مُعرّف أو قابل للتعرف عليه ... بصفة مباشرة أو غير مباشرة، لا سيما بالرجوع إلى رقم التعريف أو عنصر - أو عدة عناصر خاصة بهويته البدنية أو الفيزيولوجية أو الجينية أو البيومترية أو النفسية أو الاقتصادية أو الثقافية أو الاجتماعية"⁽⁷⁾. ويتضمن هذا القانون مجموعة من الضمانات، من بينها⁽⁸⁾:

- ضرورة الحصول على موافقة صريحة للمعالجة⁽⁹⁾،
 - تحديد أغراض جمع البيانات⁽¹⁰⁾،
 - تنظيم نقل المعطيات إلى الخارج⁽¹¹⁾،
 - إنشاء السلطة الوطنية لحماية البيانات الشخصية كهيئة مختصة بالرقابة والضبط⁽¹²⁾.
- غير أن التطبيق العملي لهذا القانون يواجه عدة تحديات، أبرزها تأخر تنصيب الهيئة الرقابية لفترة طويلة، وضعف الثقافة الرقمية لدى الأفراد، وغياب النصوص التنظيمية المكتملة.

5- التحديات التشريعية الراهنة في مجال البيئة الرقمية

رغم هذا التطور، لا يزال الحقل التشريعي لحماية البيانات يواجه تحديات جوهرية، منها:

أ. اتّساع الفجوة بين وتيرة التطور التقني وبطء الاستجابة التشريعية: ويتجلى ذلك في الاختلال المتزايد بين السرعة الهائلة التي تتطور بها التقنيات الرقمية - مثل الذكاء الاصطناعي، تحليل البيانات الضخمة، تقنيات التتبع، والحوسبة السحابية - وبين القدرة البطيئة للتشريعات على مواكبة هذه التحولات. فالتكنولوجيا تُنتج أدوات جديدة لمعالجة البيانات واستخدامها بوتيرة يومية تقريباً، بينما تحتاج القوانين إلى سنوات من الحوار، والصياغة، والمراجعة، والإقرار، مما يجعلها متأخرة عن الواقع الرقمي الفعلي.

ويؤدي هذا التأخر التشريعي إلى ظهور "فراغ قانوني" تستغله أحياناً الجهات العامة والخاصة في ممارسة أنشطة رقمية ذات تأثير على الخصوصية دون وجود قواعد دقيقة تضبطها. كما يجعل المواطن أقل حماية، ويضع القاضي أمام تحديات جديدة لم تُوضع لها حلول تشريعية مسبقة. وبالتالي، يصبح سدّ هذه الفجوة ضرورة لضمان حماية فعالة للحقوق الأساسية دون تعطيل التطور التكنولوجي.

ب. **محدودية الرقابة على الجهات الأمنية عند معالجتها للبيانات:** ذلك أنّ ضعف الآليات المؤسسية والقانونية المكلفة بمتابعة مدى التزام الأجهزة الأمنية بقواعد حماية البيانات أثناء جمعها ومعالجتها. فغالبًا ما تستفيد هذه الجهات من استثناءات واسعة بدعوى حماية الأمن الوطني، مما يؤدي إلى غياب الشفافية وعدم خضوع العمليات الرقمية الحساسة - مثل المراقبة، التحليل الخوارزمي، وتتبع الاتصالات - لرقابة فعالة من هيئات مستقلة أو قضاء متخصص. كما أن اتساع سلطات الأجهزة الأمنية في الوصول إلى البيانات، دون وجود ضوابط دقيقة أو آليات مراجعة دورية، قد يفتح المجال لإمكانية التعسف أو إساءة استخدام المعلومات، وهو ما يبرز الحاجة إلى نظام رقابي متعدد المستويات يوازن بين مقتضيات الأمن واحترام الحقوق الأساسية للمواطن.

ج. **ضعف الوعي المجتمعي بحقوق الخصوصية الرقمية:** فنسبة كبيرة من الأفراد لا تدرك طبيعة البيانات التي تُجمع عنها، ولا المخاطر المترتبة على إساءة استخدامها، ولا الحقوق التي يضمنها القانون لمهايتها. فالمستخدم العادي يتعامل مع الخدمات الرقمية - منصات التواصل، التطبيقات، الخدمات السحابية - دون قراءة شروط الاستخدام أو فهم آليات التتبع والتحليل التي تقوم بها الشركات أو الجهات الحكومية.

ويؤدي هذا النقص في الوعي إلى تساهل كبير في مشاركة المعلومات الشخصية، والقبول بممارسات رقمية قد تكون ماسة بالخصوصية، مما يُضعف أي مجهود قانوني أو تقني لحماية البيانات. كما يجعل المجتمع أقل قدرة على مساءلة المؤسسات، وأقل استعدادًا للكشف عن الانتهاكات أو المطالبة بالشفافية.

ولذلك، يرتبط بناء منظومة فعالة لحماية الخصوصية بترسيخ ثقافة رقمية قائمة على الوعي بالحقوق والواجبات، من خلال التربية الرقمية، الحملات التوعوية، ودور المؤسسات التعليمية والإعلامية في نشر ثقافة حماية البيانات.

د. **استمرار التوتر بين ضرورات الأمن الوطني ومتطلبات حماية الخصوصية:** فهو أحد الإشكالات البنوية في البيئة الرقمية الحديثة، حيث تجد الدولة نفسها مطالبة بجمع وتحليل كميات متزايدة من البيانات لحماية الأمن الوطني ومكافحة التهديدات السيبرانية والجريمة المنظمة، في حين يفرض احترام الخصوصية الرقمية قيودًا على حجم البيانات المجمعة، وأغراض استخدامها، وحدود معالجتها.

ويعود هذا التوتر إلى اختلاف طبيعة الهدفين؛ إذ يتطلب الأمن الوصول إلى المعلومات بسرعة وفعالية، بينما تتطلب الخصوصية وضع ضوابط دقيقة ومراحل تحقق واستئذان قد تُبطئ العمل الأمني أو تُقيّد فعاليته. كما أن غياب المعايير الواضحة والشفافة، أو ضعف الرقابة على الأجهزة الأمنية، يؤدي إلى اتساع دائرة الشك لدى المواطنين من احتمال إساءة استخدام البيانات، في حين ترى المؤسسات الأمنية أن القيود القانونية قد تُعيق قدرتها على مواجهة تهديدات متطورة وسريعة.

ويُنتج هذا التناقض حالة دائمة من التوازن الهش، تجعل من الضروري اعتماد مقاربة شمولية تجمع بين تطوير الأطر القانونية، وتحسين أدوات الحوكمة، وتبني حلول تقنية تقلل الحاجة لجمع البيانات الحساسة، بما يخفف حدة هذا التوتر ويمنع تحوُّله إلى تعارض بين الأمن والحقوق الأساسية.

تُبرز هذه التحديّات الحاجة إلى تحديث التشريعات بشكل مستمر واعتماد معايير تقنية وقانونية تمنع إساءة استعمال البيانات دون إضعاف قدرات الدولة في حماية أمنها.

ثانيا- حدود الحق في الخصوصية الرقمية بين الضمانات الدستورية ومتطلبات المعالجة الحديثة للبيانات

يُعدّ الحق في الخصوصية الرقمية امتداداً طبيعياً للحياة الخاصة، غير أنّ هذا الحق لم يعد مطلقاً في بيئة رقمية تتسم بتطورات تقنية متسارعة وقدرات متزايدة على جمع البيانات وتحليلها. وبينما تمنح الدساتير والقوانين الأساسية حماية لهذا الحق، تفرض المعالجة الحديثة للبيانات - خاصة عبر الذكاء الاصطناعي، الحوسبة السحابية، وتتبع السلوك الرقمي - متطلبات جديدة غالباً ما تضعه تحت ضغط الولاءات الأمنية والتنظيمية. ومن ثم، بات من الضروري تحليل حدود هذا الحق بين مبادئه الدستورية التقليدية وضرورات المعالجة في العصر الرقمي.

1- الإطار الدستوري للحق في الخصوصية الرقمية

تُجمع الدساتير الحديثة على حماية الحياة الخاصة باعتبارها حقاً أساسياً، وتشمل هذه الحماية سرّية الاتصالات⁽¹³⁾، حرمة المسكن، ومنع جمع المعلومات الشخصية دون مبرر قانوني. وقد شهدت بعض الدساتير إدماجاً صريحاً لمفهوم الخصوصية الرقمية، اعترافاً بكون الوسائط الجديدة لم تعد منفصلة عن حياة الأفراد.

وفي الجزائر، ينص دستور 2020 على حماية الحياة الخاصة، وحق كل شخص في سرّية مراسلاته واتصالاته الخاصة بكافة أشكالها. وهو ما يفهم منه ضمناً شمول هذا الحق للمراسلات والاتصالات الرقمية. وأنّ المشرّع الدستوري الجزائري قد أقرّ امتداد الحماية التقليدية إلى الفضاء الإلكتروني، وهو ما يضع إطاراً عاماً لمشروعية المعالجة الرقمية للبيانات.⁽¹⁴⁾

2- الطبيعة غير المطلقة للحق في الخصوصية الرقمية

رغم مكانة هذا الحق، فإنّ الخصوصية - رقمية كانت أم غير ذلك - حق غير مطلق ويخضع لمجموعة من القيود المشروعة.⁽¹⁵⁾ وتفرض الشرعية الدستورية ثلاثة مبادئ أساسية في كل تقييد:

- أ. مبدأ المشروعية: لا يجوز جمع أو معالجة أو تخزين البيانات إلا بناءً على نص قانوني.
- ب. مبدأ الضرورة: يجب أن يكون التقييد ضرورياً لتحقيق هدف مشروع، خاصة في مجالات الأمن الوطني وحماية النظام العام.

ج. مبدأ التناسب: يجب ألا يتجاوز تدخل الدولة الحد الأدنى اللازم لتحقيق الهدف. وتنسجم هذه المبادئ مع التوجهات الدولية، وخاصة اجتهادات المحكمة الأوروبية لحقوق الإنسان التي تشدد على ألا تكون إجراءات المراقبة الرقمية "جائرة أو غير قابلة للتوقع".⁽¹⁶⁾

3- متطلبات المعالجة الحديثة للبيانات وتحدياتها على الخصوصية الرقمية

تفرض المعالجة الحديثة للبيانات تحديات غير مسبقة على مفهوم الخصوصية، إذ إن:

أ. **الذكاء الاصطناعي** قادر على إعادة بناء ملفات شخصية دقيقة استنادًا لبيانات مجزأة أو حتى مجهولة الهوية.

ب. **البيانات الضخمة (Big Data)** تسمح بالكشف عن أنماط سلوك فردي وجماعي، مما يزيد من مخاطر التتبع والمراقبة المستمرة.

ج. **الحوسبة السحابية** تُسهّل تدفق البيانات عبر الحدود، وتُضعف قدرة البلدان النامية على مراقبة مسارات المعالجة.

د. **إنترنت الأشياء (IoT)** ينتج كميات هائلة من البيانات حول الحياة اليومية للفرد، غالبًا دون علمه الكامل أو موافقته.⁽¹⁷⁾

هذه التحولات تجعل من الصعب على التشريعات التقليدية ضبط كل حالات الجمع والمعالجة، لأن طبيعة البيانات أصبحت تنبؤية وليست مجرد معلومات ثابتة، وهو ما يوسع نطاق تدخل الدولة والقطاع الخاص في المساحة الشخصية للفرد.

4- متطلبات المعالجة الحديثة للبيانات وتحدياتها على الخصوصية الرقمية

تدخل الدولة في المجال الرقمي غالبًا ما يرتبط بضرورات مكافحة الإرهاب، تتبع الجرائم الإلكترونية، حماية البنى التحتية الحساسة، ومواجهة الهجمات السيبرانية.⁽¹⁸⁾ وبموجب هذه الضرورات، تمنح التشريعات - بما فيها الجزائية - استثناءات على قاعدة حماية الخصوصية، مثل:

أ. الترخيص للجهات الأمنية بالوصول إلى البيانات الحساسة في إطار أوامر قضائية أو عمليات استخباراتية.

ب. جمع البيانات الميتا (Metadata) الخاصة بالاتصالات لتحديد الأنماط دون الكشف المباشر عن المحتوى.

ج. مراقبة حركة البيانات عبر الشبكات الوطنية لضمان الأمن السيبراني.

غير أن التوسع غير المنضبط في هذه الاستثناءات قد يؤدي إلى "مراقبة شاملة" تهدد جوهر الحق في الخصوصية. ولهذا تشدد المعايير الدولية على ضرورة إحاطة كل ممارسة أمنية بضمانات: كتابة، واضحة، متوقعة، وشفافة، مع إخضاعها لرقابة قضائية ومؤسسية مستقلة.

4- متطلبات المعالجة الحديثة للبيانات وتحدياتها على الخصوصية الرقمية

أضحى التوفيق بين ضمانات الخصوصية ومتطلبات المعالجة الحديثة للبيانات يقتضي - نموذجًا جديدًا يقوم على:

على:

- أ. إدراج حماية الخصوصية ضمن التصميم التقني. (Privacy by Design).
 - ب. استخدام تقنيات إخفاء الهوية والخصوصية التفاضلية للحد من المخاطر فيما يتعلق بالبيانات الضخمة.
 - ج. تعزيز الشفافية بشأن ما يُجمع من بيانات وكيفية استعمالها وأغراضها الأمنية أو الإدارية.
 - د. اعتماد حكمة رقمية فعالة تُخضع الجهات المعالجة للمساءلة، خاصة هيئات الأمن المكلفة بتسيير بيانات واسعة النطاق.
 - هـ. تقوية دور الهيئات الوطنية المستقلة، مثل السلطة الوطنية لحماية البيانات في الجزائر، في مراقبة امتثال الجهات المعالجة للضمانات القانونية.
- وهذا يتضح أن حدود الخصوصية الرقمية لم تعد تُحدّد فقط بنصوص الدستور، وإنما بطبيعة التكنولوجيا المعتمدة، والممارسات الأمنية، ومستوى نضج الإطار التنظيمي والتقني للدولة.

المحور الثاني: الأمن الوطني بين ضرورات جمع البيانات واستشراف المستقبل الرقمي

أضحى الأمن الوطني في العصر الرقمي يعتمد بشكل متزايد على قدرات الدولة في جمع البيانات وتحليلها وتوظيفها ضمن منظومات تقنية متطورة، لاسيما مع تنامي التهديدات السيبرانية وازدياد تعقيد الجرائم المرتبطة بالفضاء الإلكتروني. وقد أتاح التطور السريع في تقنيات الذكاء الاصطناعي والبيانات الضخمة للدول إمكانات واسعة لتعزيز مراقبة المخاطر والتنبؤ بها، غير أنّ هذا التوسع في أدوات الرصد والتحليل يثير إشكالات قانونية وأخلاقية عميقة تتعلق بمدى احترام الخصوصية الرقمية وحدود التدخل في الحياة الشخصية للأفراد. وفي ظل هذا الواقع المتشابك، تبرز الحاجة إلى دراسة الدور الاستراتيجي لهذه التقنيات في دعم المنظومات الأمنية من جهة، واستكشاف آفاق إرساء توازن واقعي بين مقتضيات الأمن وضمانات الخصوصية من جهة أخرى، بما يستند إلى حلول تقنية مبتكرة وحكمة رقمية رشيدة قادرة على ضمان الأمن دون المساس بالحقوق الجوهرية.

أولا- دور الذكاء الاصطناعي والبيانات الضخمة في دعم المنظومات الأمنية وتحدياتها القانونية

أصبحت التقنيات الرقمية المتقدمة—وفي مقدمتها الذكاء الاصطناعي والبيانات الضخمة—ركيزة أساسية في عمل المنظومات الأمنية الحديثة، لما توفره من قدرات واسعة على جمع المعلومات وتحليلها والتنبؤ بالتهديدات. ومع ذلك، يثير هذا التطور أسئلة قانونية دقيقة تتعلق بمدى مشروعية الاستخدام، وضوابط المعالجة، واحترام الحقوق الأساسية وفي مقدمتها الخصوصية الرقمية. ومن ثم، فإنّ تحليل دور هذه التقنيات يستدعي الوقوف عند مزاياها الأمنية من جهة، وتحدياتها القانونية من جهة أخرى.

1- الذكاء الاصطناعي كأداة لتعزيز الفعالية الأمنية

يعدّ الذكاء الاصطناعي أحد أهم الأدوات التي اعتمدت عليها الدول في تطوير أنظمتها الأمنية، نظرا لقدراته في معالجة كميات كبيرة من البيانات بطريقة تفوق القدرات البشرية. وتبرز أهم استخداماته في المجال الأمني في⁽¹⁹⁾:

- أ. الكشف الاستباقي عن التهديدات: من خلال تحليل أنماط السلوك الرقمي والتعرف على الأنشطة غير العادية التي قد تشير إلى هجمات سببرانية أو عمليات إجرامية.
- ب. التعرف على الهوية باستخدام تقنيات التعرف على الوجوه (Facial Recognition) والبصمة السلوكية، مما يسهم في تتبع المطلوبين ومراقبة الأماكن العامة.
- ج. إدارة الأزمات والكوارث عبر قراءة البيانات الزمنية في الوقت الحقيقي، وتقديم توقعات لحظية تساعد الأجهزة الأمنية على اتخاذ قرارات دقيقة.
- د. تحليل الاتصالات ووسائل التواصل لاستخراج المؤشرات المتعلقة بجرائم الإرهاب والتطرف العنيف.

لذا فإنّ الأنظمة الأمنية في العديد من الدول أصبحت تعتمد الذكاء الاصطناعي في ما يُعرف بـ الأمن الاستباقي (Predictive Security)، الذي يقوم على التنبؤ بالتهديد قبل وقوعه، وليس فقط التعامل نتائجها. (20)

2- البيانات الضخمة ودورها في بناء منظومات أمنية متكاملة

تشكل البيانات الضخمة (Big Data) الأساس الحيوي للذكاء الاصطناعي، وهي تتضمن كميات هائلة من البيانات المتدفقة من مختلف المصادر، مثل الاتصالات، منصات التواصل الاجتماعي، أجهزة الاستشعار، كاميرات المراقبة، خدمات تحديد الموقع، والمعاملات الإلكترونية. وقد مكّنت هذه البيانات الأجهزة الأمنية من:

- أ. تحليل أنماط السلوك الإجرامي وتحديد البؤر الجغرافية الأكثر عرضة للمخاطر.
- ب. مراقبة الشبكات الإجرامية وتوقع تحركاتها عبر تحليل العلاقات الرقمية (Network Analysis).
- ج. التعرف على الهجمات السببرانية من خلال تحليل السلوك الشبكي واكتشاف المؤشرات الشاذة.
- د. دعم حملات مكافحة الإرهاب عبر تحليل البيانات العابرة للحدود المتعلقة بالتنقل، التحويلات المالية، النشاط الإلكتروني، إلخ.

وتعتبر هذه الوظائف جوهرية في تطوير مفهوم الأمن السببراني الوطني، الذي يعتمد على تحليل ضخم ومتعدد الطبقات للبيانات من أجل حماية البنى التحتية الحيوية.

3- التحديات القانونية المرتبطة باستخدام الذكاء الاصطناعي والبيانات الضخمة

على الرغم من الفوائد الأمنية الكبيرة لهذه التقنيات، فإنّ استخدامها يطرح تحديات قانونية كبرى، من أبرزها:

- أ. مخاطر المساس بالخصوصية الرقمية

تعتمد الخوارزميات الأمنية على جمع بيانات واسعة، غالبًا دون علم الأفراد أو بموافقة شكلية لا تعكس استيعابًا حقيقيًا لطبيعة المعالجة⁽²¹⁾. وتشمل هذه البيانات:

- الصور الحيوية (Biometrics)،
- البيانات السلوكية،
- بيانات الموقع الجغرافي،
- البيانات الوصفية (Metadata).

وتمثل هذه البيانات في مجموعها قدرة على "إعادة بناء شخصية الفرد الرقمية"، مما يثير التساؤل حول مدى إمكانية التوفيق بين الأمن وحماية الخصوصية.

ب. إشكالية الشفافية والخوارزميات السوداء (Black Box)

تتميز أنظمة الذكاء الاصطناعي غالبًا بكونها غير شفافة، إذ يصعب معرفة المعايير التي تعتمدها في اتخاذ القرارات. ويخلق ذلك عدة مخاطر:

- صعوبة الطعن في القرارات الأمنية المبنية على الخوارزميات.
- احتمال تشكل تحيزات خوارزمية تؤدي إلى ممارسات تمييزية.
- غياب الرقابة القضائية الدقيقة على عمليات التحليل الأمني.

ج. غياب إطار قانوني شامل

في العديد من الدول - ومنها الجزائر - لا يزال الإطار القانوني المنظم للذكاء الاصطناعي والبيانات الضخمة في المجال الأمني في طور التشكل. فرغم وجود قانون حماية البيانات (18-07) الذي يضع قواعد عامة، تبقى الحاجة ملحة إلى:

- نصوص خاصة تنظم استخدام الذكاء الاصطناعي في القطاعات الحساسة،
- تحديد معايير الشفافية والمساءلة،
- ضبط حدود تدخل الأجهزة الأمنية عند جمع وتحليل البيانات،
- تجريم إساءة استخدام البيانات التحليلية لأغراض خارج نطاق الأمن الوطني.

4 - الحاجة إلى ضمانات قانونية مصاحبة للاستخدام الأمني للتقنيات المتقدمة

توصي الأدبيات الدولية بضرورة وضع ضمانات قانونية وتقنية تُحاصر مخاطر التوسع الأمني في استخدام هذه الأدوات، من أهمها⁽²²⁾:

- أ. إخضاع كل معالجة أمنية للبيانات لمبدأ الضرورة والتناسب.
- ب. فرض تقييمات أثر أمنية وقانونية قبل اعتماد أي نظام ذكاء اصطناعي.
- ج. تعزيز رقابة الهيئات الوطنية لحماية البيانات على الأنظمة الأمنية، بما في ذلك سلطة البيانات في الجزائر.

د. وضع قواعد واضحة للحكومة للخوارزمية (Algorithmic Governance)

هـ. تطوير تقنيات تقلل من الكشف عن هوية الأفراد-(De-identification & Privacy preserving).

و. وبذلك يتضح أن الذكاء الاصطناعي والبيانات الضخمة أصبحا عنصرين مركزيين في بناء منظومة أمنية فعالة، غير أن استخدامهما دون ضوابط قانونية صارمة يمكن أن يؤدي إلى توسع رقابي يهدد جوهر الحقوق الأساسية، وعلى رأسها الخصوصية الرقمية.

ثانيا- آفاق تحقيق التوازن بين الخصوصية والأمن من خلال الحلول التقنية والحكمة الرقمية

يُعتبر البحث عن صيغة متوازنة تجمع بين حماية الخصوصية الرقمية وضمان الأمن الوطني أحد أكثر التحديات تعقيداً في البيئة الرقمية المعاصرة. فالتوسع المتزايد في استخدام البيانات، والاعتماد المكثف على الذكاء الاصطناعي في تحليلها، وضع صانعي السياسات أمام معادلة دقيقة تتطلب التفكير في آليات جديدة تتجاوز المقاربات القانونية التقليدية، وتستند إلى حلول تقنية مبتكرة وأطر متقدمة للحكمة الرقمية. ويظهر هذا التوازن كخيار استراتيجي لا يهدف فقط إلى معالجة التوتر بين الأمن والخصوصية، بل إلى وضع نموذج شمولي يضمن حماية الحقوق الأساسية دون الإضرار بفعالية المنظومات الأمنية.

1- الحلول التقنية الضامنة للخصوصية كمدخل لتحقيق التوفيق بين الحقوق ومتطلبات الأمن

أضخى إدماج أدوات تقنية متقدمة في عمليات جمع البيانات ومعالجتها أحد المسارات الأساسية لتحقيق توازن واقعي بين متطلبات الأمن والخصوصية. فالتطورات الحديثة في مجال أمن المعلومات مكنت من ابتكار آليات تسمح للدولة بالحصول على البيانات الضرورية لحماية النظام العام دون تعريض الحقوق الشخصية للاختراق أو الاستغلال غير المشروع.

أ. تقنيات التعمية (التشفير) Encryption وتقليل نطاق البيانات Data Minimization

تعدّ التعمية من أقوى الوسائل لحماية سرية البيانات أثناء معالجتها أو تداولها بين مختلف الهيئات الأمنية⁽²³⁾. إذ تسمح للدولة بالاحتفاظ بقدرة تحليل البيانات في إطار مكافحة الجرائم السيبرانية، مع ضمان بقاء هوية الأفراد أو محتوى البيانات الحساسة غير قابل للاطلاع من قبل غير المخول لهم. كما تشكل سياسة "تقليل البيانات" أحد المبادئ الحديثة التي تفرض جمع الحد الأدنى الضروري من المعلومات، بما يحد من مخاطر المراقبة الواسعة أو التعسف الرقمي⁽²⁴⁾.

ب. الخصوصية التفاضلية Differential Privacy والحوسبة متعددة الأطراف الآمنة Secure

Multi-Party Computation

أفرزت البحوث الحديثة في علوم البيانات حلولاً أكثر تطوراً تُتيح للجهات الأمنية إجراء تحليلات شاملة على مجموعات البيانات دون الكشف عن الهويات الفردية. وتعد الخصوصية التفاضلية مثالاً واضحاً لهذا الاتجاه، إذ تسمح باستخراج الأنماط الإحصائية التي تفيد الأجهزة الأمنية دون إمكانية إرجاع النتائج إلى شخص معين. أما الحوسبة متعددة الأطراف الآمنة فتمكّن عدة جهات من معالجة بيانات مشتركة دون اطلاع أي طرف على البيانات الخام، وهو ما يوفر درجة عالية من حماية الخصوصية حتى في العمليات الرقمية الحساسة⁽²⁵⁾.

ج. بنى الهوية الرقمية القائمة على اللامركزية (Blockchain-based ID Systems)

فتحت تقنيات البلوكتشين آفاقاً واسعة لإنشاء نظم هويات رقمية آمنة تمنح الأفراد قدرة أكبر على التحكم في بياناتهم، وتحدّ من مخاطر إساءة استخدامها. إذ تسمح هذه الأنظمة بتحقيق عمليات تحقق أمنية فعالة دون الحاجة إلى تخزين بيانات المستخدمين لدى جهة مركزية قد تكون عرضة للاختراق أو الاستغلال⁽²⁶⁾.

2- الحكامة الرقمية كإطار لتحقيق التوازن بين الأمن والحقوق الأساسية

لا يكفي الاعتماد على الحلول التقنية وحدها لضمان حماية الخصوصية في عصر الأمن السيبراني، بل يتعين تبني نموذج متكامل للحكامة الرقمية قادر على تنظيم استخدام البيانات بما ينسجم مع متطلبات الشفافية والمساءلة وسيادة القانون. وتمثل الحكامة الرقمية في مجموعة من المبادئ والآليات التي تضمن إدارة البيانات بمسؤولية، وتحدد بدقة نطاق تدخل الدولة والجهات الأمنية⁽²⁷⁾.

أ. الشفافية والمساءلة في جمع البيانات واستخدامها

تعتبر الشفافية الركيزة الأولى لضمان الثقة العامة في المؤسسات الأمنية، إذ إن تحديد الأغراض بدقة، وتوضيح أساليب المعالجة، وتوفير آليات للاعتراض، كلها جوانب تركز الحق في الخصوصية دون المساس بفعالية العمل الأمني⁽²⁸⁾. كما تسهم آليات المراجعة الدورية للسياسات الأمنية، وإخضاعها لرقابة برلمانية وقضائية، في الحد من التجاوزات المحتملة وضمان التناسب في التدخل.

ب. الرقابة متعددة المستويات والهيئات المستقلة لحماية البيانات

أثبتت التجارب الدولية أن إسناد مهمة مراقبة التزام الجهات الأمنية بمعايير حماية البيانات إلى هيئات مستقلة يمثل عنصراً محورياً في الحكامة الرقمية⁽²⁹⁾. وتعمل هذه الهيئات على فحص آليات المعالجة الأمنية للبيانات، والتأكد من احترام مبادئ الضرورة والتناسب، إضافة إلى تلقي الشكاوى والتحقيق في الانتهاكات. كما تسمح الرقابة متعددة المستويات - القضائية، البرلمانية، والإدارية - بخلق منظومة تضمن عدم تغول السلطات الرقمية.

ج. استشراف أخلاقيات الذكاء الاصطناعي وتبني مبادئ "الاستخدام المسؤول"

إن إدماج الذكاء الاصطناعي في العمل الأمني لا يخلو من مخاطر تتعلق بالتمييز الخوارزمي، أو اتخاذ قرارات آلية غير مبررة تمس الحقوق الأساسية⁽³⁰⁾. لذا، تزايدت الحاجة إلى تبني مبادئ أخلاقيات الذكاء الاصطناعي، مثل العدالة، الشفافية، وإمكانية تفسير القرارات، وهي مبادئ بدأت بعض التشريعات - كالتشريع الأوروبي - في إدراجها صراحة ضمن أدوات تنظيم الأمن السيبراني⁽³¹⁾.

د. بناء ثقافة رقمية مجتمعية قائمة على الوعي بالحقوق والواجبات

يمثل الوعي الرقمي عنصراً أساسياً لإنجاح أي مقارنة تسعى إلى التوفيق بين الخصوصية والأمن⁽³²⁾. فتمكين الأفراد من فهم كيفية عمل المنظومات الأمنية الرقمية، وطبيعة البيانات التي يتم جمعها، والحقوق التي يكفلها القانون لهم، يساعد في الحد من المخاوف المجتمعية تجاه المراقبة الرقمية. كما يساهم ذلك في تعزيز التعاون بين المواطن والدولة في مواجهة التهديدات السيبرانية.

يتبين أن تحقيق التوازن بين الخصوصية والأمن لم يعد مسألة تتعلق فقط بالحدود القانونية للتدخل الأمني، بل أصبح مشروعاً متعدد الأبعاد يستند إلى حلول تقنية متقدمة، وأطر حكام رقمية رشيدة، وسياسات تشريعية قادرة على التكيف المستمر مع التحولات الرقمية⁽³³⁾. ويشكل هذا التوازن ليس فقط ضرورة حقوقية، بل خياراً استراتيجياً لدعم الأمن الوطني بشكل فعال ومستدام، دون المساس بالحقوق الأساسية للمواطن الرقمي.

خاتمة:

يتضح من خلال هذه القراءة أن مستقبل الخصوصية الرقمية والأمن الوطني مرهون بمدى قدرة المشرع والمؤسسات على تطوير مقاربة متكاملة تراعي الطبيعة المتغيرة للتقنيات الرقمية، وتضمن حماية الحقوق الأساسية دون تعطيل فعالية المنظومات الأمنية. فالرهان الحقيقي يكمن في بناء بيئة تشريعية مرنة، مدعومة بأدوات تقنية موثوقة، وبثقافة رقمية مجتمعية تضع الفرد في صميم العملية الإصلاحية، بما يسمح بتحقيق الأمن مع صون الكرامة الرقمية. وانطلاقاً من هذا التحليل، تم التوصل إلى جملة النتائج والتوصيات العملية الداعمة لهذا التوازن المنشود.

أولاً: النتائج

1. **تزايد مركزية البيانات الرقمية:** أثبتت الدراسة أن البيانات الرقمية أصبحت تمثل مورداً استراتيجياً للدول، مما جعل الخصوصية الرقمية أكثر هشاشة أمام توسع أدوات المراقبة وتحليل البيانات.
2. **قصور الإطار التشريعي التقليدي:** فالتشريعات الحالية - خاصة في الدول النامية - لا تزال عاجزة عن مواكبة التحولات التقنية، مما يخلق فراغاً قانونياً بين حماية الحقوق ومتطلبات الأمن الوطني.
3. **تناهي تدخل الدولة في المجال الرقمي:** فالحاجة الأمنية دفعت الدول إلى تعزيز آليات جمع البيانات، لكن ذلك يتم في كثير من الأحيان دون وضع ضمانات قانونية وتقنية كافية للحد من التعسف.
4. **صعود الذكاء الاصطناعي والبيانات الضخمة:** فالتقنيات الحديثة تؤدي إلى تعزيز قدرات أجهزة الأمن، لكنها في الوقت ذاته تزيد من مخاطر اختراق الخصوصية وتهديد مبدأ الحد الأدنى من المعالجة.
5. **إمكانية تحقيق توازن معقول:** حيث بينت الدراسة أن تحقيق التوازن بين الخصوصية والأمن ليس مستحيلاً، شريطة اعتماد مقاربة تدمج بين الإصلاح التشريعي، والحلول التقنية، وحكام البيانات، والوعي المجتمعي.

ثانياً: التوصيات

1. **تحديث الإطار التشريعي الوطني** من خلال اعتماد قوانين شاملة لحماية البيانات تتماشى مع المعايير الدولية (مثل الـGDPR)، مع ضمان وضوح شروط جمع البيانات، مدة الاحتفاظ، وإجراءات الطعن.

2. تعزيز الرقابة المؤسسية والقضائية بإنشاء هيئات مستقلة فعالة لمراقبة معالجة البيانات ذات الطابع الأمني، وتمكين القضاء من ممارسة رقابة صارمة على مشروعية التدخل الرقمي.
3. تطوير حلول تقنية ضامنة للخصوصية مثل: التعمية (التشفير)، تقنيات إخفاء الهوية (Anonymization)، تقليل البيانات (Data Minimization)، والخصوصية التفاضلية (Differential Privacy).
4. ترقية منظومات الأمن السيبراني من خلال الاستثارة في بنى تحتية رقمية آمنة، واعتماد حلول الذكاء الاصطناعي القابلة للتفسير (Explainable AI) للحد من انحياز الخوارزميات.
5. تعزيز الوعي الرقمي للمواطن من خلال وضع برامج وطنية للتوعية بمخاطر مشاركة البيانات، الحقوق الرقمية، وإجراءات الحماية الذاتية في الفضاء الإلكتروني.
6. تبني مقاربة توازن مستدام يقوم على مبادئ: الضرورة، التناسب، المشروعية، الشفافية، وتقييم الأثر على البيانات (DPLA) قبل أي مشروع أمني رقمي جديد.

الهوامش والمراجع:

(1) - مجلس أوروبا، اتفاقية حماية الأشخاص تجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي- (1981)، مجموعة المعاهدات الأوروبية، رقم 108، وثيقة مترجمة في إطار برنامج تعزيز الإصلاح الديمقراطي في دول جنوب المتوسط، ستراسبورغ، 28 يناير 1981.

(2) - European Union, REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, 4.5. 2016 L 119/1, EUR-Lex, Access to European Union Law. Link: <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>, Checked on 11-11-2024, At 19:45.

(3) - OECD, Recommendation of the Council concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (2025), Link: <https://legalinstruments.oecd.org/public/doc/114/114.en.pdf>, Checked on 11-11-2025, At 20:30.

(4) - قرار الجمعية العامة للأمم المتحدة رقم A/RES/69/66 الصادر في 18 كانون الأول/ديسمبر 2014، الحق في الخصوصية في العصر الرقمي، الرابط: <https://docs.un.org/ar/a/res/69/166>. تم الاطلاع على الوثيقة بتاريخ 11-11-2025، الساعة 21:00.

(5) - Convention on Cybercrime, Budapest, 23.XI.2001, European Treaty Series- No. 185, Council of Europe, Link: <https://rm.coe.int/1680081561>, Checked on 12-11-2025, At 11:15.

الحق في الخصوصية الرقمية بين حماية البيانات ومتطلبات الأمن الوطني: قراءة استشرافية
عبد الرزاق صحراوي - خليل سلطاني

(6) - اتفاقية الأمم المتحدة لمكافحة الجريمة السيبرانية الموقعة بنيويورك عام 2024، تعزيز التعاون الدولي لمكافحة جرائم معينة مرتكبة بواسطة نظم تكنولوجيا المعلومات والاتصالات ولتبادل الأدلة في شكل إلكتروني على الجرائم الخطيرة، مكتب الأمم المتحدة المعني بالمخدرات والجريمة، الرابط: https://treaties.un.org/doc/Treaties/2024/12/20241224%2001-27%20PM/Ch_XVIII_16.pdf، تم الاطلاع على الوثيقة بتاريخ 21-11-2025، الساعة 11:30.

(7) - الفقرة الأولى من المادة 3 من القانون رقم 07-18 المؤرخ في 10 يونيو 2018 بشأن حماية الأشخاص الطبيعيين في معالجة البيانات ذات الطابع الشخصي، الجريدة الرسمية للجمهورية الجزائرية، العدد 34، الصادر في 10 يونيو 2018.

(8) - المصدر نفسه.

(9) - الفقرة الثانية من المادة 7، المصدر نفسه.

(10) - الفقرة الثانية من المادة 10، المصدر نفسه.

(11) - المادتان 44 و 45 من الفصل الرابع المعنون "نقل المعطيات إلى دولة أجنبية" من الباب الخامس المعنون "التزامات المسؤول عن المعالجة، المصدر نفسه.

(12) - الباب الثالث المعنون "السلطة الوطنية لحماية المعطيات ذات الطابع الشخصي"، المواد من 22 إلى 31، المصدر نفسه.

(13) - المادة 10 من القانون الأساسي لجمهورية ألمانيا الاتحادية، ترجمة مؤسسة فريدريش إيبيرت، طبعة تموز 2002، الرابط: https://dalil.de/wp-content/uploads/2018/09/grundgesetz_Arabic.pdf، تم الاطلاع على الوثيقة بتاريخ 22-11-2025، الساعة 10:15.

(14) - المادة 47 من دستور الجمهورية الجزائرية الديمقراطية الشعبية، الصادر بالجريدة الرسمية للجمهورية الجزائرية، العدد 82، بتاريخ 30 ديسمبر 2020.

(15) - European court of Human Rights, Case of Roman ZAKHAROV v. Russia, Application n° 47143/06, December 4th, 2015, Link: <https://hudoc.echr.coe.int/fre?i=001-159324>, Checked on 22-11-2025, at 16^h:00^{mn}.

(16) - Ibid.

(17) - يشير إنترنت الأشياء إلى شبكة من الأجهزة الذكية المتصلة بالإنترنت، تتيح لها التواصل فيما بينها ومع السحابة الإلكترونية، وجمع البيانات عبر أدوات الاستشعار ومعالجتها للاستجابة بكفاءة لاحتياجات المستخدم، بفضل تطور رقائق الحاسوب منخفضة التكلفة وتوسع شبكات الاتصال عالية السرعة. انظر - موقع *AWS MarketPlace*، "ما المقصود بإنترنت الأشياء (IoT)؟"، الرابط:

<https://aws.amazon.com/ar/what-is/iot/>، تم الاطلاع بتاريخ : 22-11-2025، الساعة: 16:10.

(18) – إليزابيث برو، السلامة السيبرانية: اتجاهات تصاعد "الجريمة الرقمية" ضد البنية التحتية للبول، مقال منشور على موقع المستقبل للأبحاث والدراسات المتقدمة، بتاريخ 11 ديسمبر 2025، الرابط: <https://shorturl.at/GbvQ1>، تم الاطلاع بتاريخ : 03-01-2026، الساعة 17:45.

(19)– OECD, AI Principles, Link: <https://www.oecd.org/en/topics/ai-principles.html>, Checked on 22-11-2025, At: 17^h:45^{mn}.

(20)– UNICRI & INTERPOL, Artificial Intelligence and Robotics for Law Enforcement, Link: <https://www.europarl.europa.eu/cmsdata/196207/UNICRI%20-%20Artificial%20intelligence%20and%20robotics%20for%20law%20enforcement.pdf>, Checked on 22-11-2025, At: 17^h:55^{mn}.

(21)– European court of Human Rights, Case of S. and MARPER v. THE UNITED KINGDOM, Application n° 30562/04 and 30566/04, Grand Chamber, STRASBOURG, December 4th, 2008, Link: <https://hudoc.echr.coe.int/fre?i=001-90051>, Checked on 22-11-2025, at 18^h:00^{mn}.

(22)- Benjamin Raue; Antje von Ungern-Sternberg And others, Artificial Intelligence and Fundamental Rights: The AI Act of the European Union and its implications for global technology regulation, article published in ([Schriften des IRDT Trier Studies on Digital Law](https://www.schriften-des-irdt-trier.de/)) Website, Link: <https://irdt-schriften.uni-trier.de/index.php/irdt/index>, Checked on 23-11-2025 at 18^h:30^{mn}.

(23)- Bruce SCHNEIER, Data and Goliath : The Hidden Battles to Collect Your Data and Control Your World, W.W. NORTON & COMPANY, New York, London, P. 122, Link: https://ciberativismoeguerra.wordpress.com/wp-content/uploads/2017/09/bruce-schneier-data-and-goliath_-2015.pdf, Checked on 23-11-2025 at 18^h:15^{mn}.

(24)- Benjamin Raue; Antje von Ungern-Sternberg And others, Artificial Intelligence and Fundamental Rights: The AI Act of the European Union and its implications for global technology regulation, ([Schriften des IRDT Trier Studies on Digital Law](https://www.schriften-des-irdt-trier.de/)) Website, Link: <https://irdt-schriften.uni-trier.de/index.php/irdt/index>, Checked on 23-11-2025 at 18^h:30^{mn}.

(25)- Cynthia DWORK and Aaron ROTH The Algorithmic Foundations of Differential Privacy, Foundations and Trends in Theoretical Computer Science, Vol. 9, Nos. 3-4

(2014), P. 5., Link: <https://www.cis.upenn.edu/~aaroht/Papers/privacybook.pdf>,
Checked on 23-11-2025 at 09^h:10^{mn}.

(26)- Don TAPSCOTT and Alex TAPSCOTT, Blockchain Revolution : How the
Technology Behind Bitcoin is changing Money, Business, and the World, An
imprint of Penguin Random House LLC 375 Hudson Street New York, 10014,
Version_1, 2016, P. 51, link: [https://itig-iraq.iq/wp-
content/uploads/2019/05/Blockchain_Revolution.pdf](https://itig-iraq.iq/wp-content/uploads/2019/05/Blockchain_Revolution.pdf), Checked on 23-11-2025 at
10^h:20^{mn}.

(27) — منظمة منظمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو)، مبادئ توجيهية لحماية حرية التعبير والحصول على المعلومات في حوكمة
المنصات الرقمية نهج متعدد الأطراف، مؤلف جماعي، ترجمة *TRADUCTEO*, 2023، ص 7. الرابط:
<https://unesdoc.unesco.org/ark:/48223/pf0000387384>، تم الاطلاع بتاريخ: 23-11-2025، الساعة:

11:10

(28)- ARTICLE 29 Data Protection Working Party, Guidelines on Transparency
under regulation 2026/679, adopted on 29 November 2017, As last revised and
adopted on 11 April 2018, Introduction, Paragraph 2, PP. 4, link:
https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_en.pdf , Checked
on 23-11-2025 at 11^h:25^{mn}.

(29)- Ibid.

(30)- Anna JOBIN, Marcello IENCA & Effy VAYENA, The global landscape of AI
ethics guidelines, article Published in nature machine intelligence website, on 02
September 2019, Link: <https://www.nature.com/articles/s42256-019-0088-2>,
Checked on 23-11-2025 at 11^h:40^{mn}.

(31)- European Commission, Ethics guidelines for trustworthy AI, Shaping Europe's
digital future, Publication 8 April 2019, Link: [https://digital-
strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai](https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai), Checked on 23-11-
2025 at 11^h:40^{mn}.

(32)- World Economic Forum, Digital Identity: Privacy, Agency and Trust, Link:
[https://intelligence.weforum.org/topics/a1G0X000005JJGcUAO/key-
issues/a1G0X000006NupJUAS](https://intelligence.weforum.org/topics/a1G0X000005JJGcUAO/key-issues/a1G0X000006NupJUAS) , Checked on 23-11-2025 at 14h:00mn.

(33)- Ibid.

