

التضليل السيبراني وهندسة الإدراك الرقمي: نحو إعادة بناء الحماية القانونية لنزاهة المعلومات والسيادة الإدراكية في عصر الذكاء الاصطناعي

الدكتور: يونس مليح

أستاذ محاضر مؤهل بجامعة مولاي إسماعيل – مكناس - كلية العلوم القانونية والسياسية بالرشيدية
عضو فريق البحث في الدراسات القانونية والاجتماعية والسياسية

y.maleh@umi.ac.ma

ملخص:

لم يعد التضليل السيبراني مجرد امتداد رقمي للأخبار الزائفة أو الدعاية التقليدية، بل أصبح أحد أكثر المخاطر المركبة التي تواجه الدولة والمجتمع في البيئة الرقمية، بالنظر إلى تداخله مع الأمن السيبراني والذكاء الاصطناعي والخوارزميات والمنصات الرقمية والأمن الرقمي. وتزداد خطورة الظاهرة بفعل الانتشار العالمي للاتصال الرقمي؛ إذ بلغ عدد مستخدمي الإنترنت سنة 2025 نحو 6 مليارات شخص، أي ما يعادل 74% من سكان العالم، مقابل 5.8 مليارات سنة 2024، في وقت بات فيه الذكاء الاصطناعي التوليدي قادراً على إنتاج النصوص والصور والأصوات والمقاطع المصطنعة وتخصيصها وتوزيعها بوتيرة غير مسبوقة (International Telecommunication Union [ITU], 2025).

ينطلق هذا المقال من فرضية أساسية مؤداها أن التضليل السيبراني لم يعد يستهدف صحة المعلومة فحسب، وإنما أصبح يستهدف البنية التي يتشكل داخلها الإدراك والثقة والقرار، الأمر الذي يبرر الانتقال من مفهوم حماية المعلومات بمعناها التقني إلى مفهوم أوسع لـ«نزاهة البيئة المعلوماتية» و«السيادة الإدراكية». وتعتمد الدراسة منهجاً تحليلياً ومقارناً بالاستناد إلى التشريع الأوروبي وتقارير وكالة الاتحاد الأوروبي للأمن السيبراني، وجهاز العمل الخارجي للاتحاد الأوروبي، ومنظمة التعاون والتنمية في الميدان الاقتصادي، والأمم المتحدة، واليونسكو، ومجلس أوروبا، إلى جانب الاستراتيجية الوطنية للأمن السيبراني بالمغرب. وتكشف الدراسة أن جهاز العمل الخارجي للاتحاد الأوروبي رصد خلال سنة 2024 أكثر من 500 حادثة مرتبطة بالتلاعب والتدخل المعلوماتي الأجنبي، شملت ما لا يقل عن 25 منصة رقمية وحوالي 38 ألف حساب، واستهدفت 322 منظمة وامتدت إلى 90 دولة (European External Action Service [EEAS], 2025). كما أصبحت وكالة الاتحاد الأوروبي للأمن السيبراني تصنف التلاعب بالمعلومات والتدخل ضمن التهديدات السيبرانية الرئيسية (European Union Agency for Cybersecurity [ENISA], 2024).

وتخلص الدراسة إلى أن فعالية المواجهة القانونية لا تكمن في إنشاء رقابة على «الحقيقة»، وإنما في بناء حكمة قائمة على المخاطر تركز على السلوك التلاعب المنظم، وشفافية الخوارزميات، وأصالة المحتوى، ومسؤولية المنصات، والولوج إلى البيانات، والتربية الإعلامية، والرقابة القضائية، مع ضرورة إدماج نزاهة البيئة المعلوماتية تدريجياً ضمن سياسات الأمن السيبراني الوطنية. الكلمات المفتاحية: التضليل السيبراني؛ السيادة الإدراكية؛ الأمن السيبراني؛ نزاهة المعلومات؛ الذكاء الاصطناعي؛ التزييف العميق؛ المنصات الرقمية؛ الأمن الرقمي؛ التلاعب بالمعلومات.

Cyber Disinformation and the Engineering of Digital Perception: Towards Reconstructing the Legal Protection of Information Integrity and Cognitive Sovereignty in the Age of Artificial Intelligence

Dr. Youness Maleh

Associate Professor at Moulay Ismail University in Meknes

Faculty of Legal and Political Sciences in Rachidia

Member of the Research Team in Legal, Social, and Political Studies

Abstract

Cyber disinformation is no longer merely a digital extension of fake news or traditional propaganda. It has become a complex systemic risk at the intersection of cybersecurity, artificial intelligence, algorithmic systems, digital platforms and democratic security. The scale of this challenge has increased with global connectivity: in 2025, approximately 6 billion people, or 74% of the world's population, were online, compared with 5.8 billion in 2024 (International Telecommunication Union [ITU], 2025). At the same time, generative artificial intelligence has substantially reduced the cost and increased the scale of producing, personalising and disseminating synthetic text, images, audio and video.

This article argues that contemporary cyber disinformation no longer targets only the accuracy of individual pieces of information; it increasingly targets the informational environment through which perception, trust and decision-making are constructed. This transformation requires moving beyond the traditional technical understanding of information security towards broader concepts of "information integrity" and "cognitive sovereignty".

Using analytical and comparative approaches, the study examines the regulatory experience of the European Union and international frameworks developed by the European Union Agency for Cybersecurity, the European External Action Service, the OECD, the United Nations, UNESCO and the Council of Europe, while also considering Morocco's National Cybersecurity Strategy.

The study highlights that more than 500 Foreign Information Manipulation and Interference incidents were documented in 2024, involving at least 25 platforms and approximately 38,000 accounts, targeting 322 organisations across 90 countries (European External Action Service [EEAS], 2025). ENISA has also recognised information manipulation and interference as part of the contemporary cybersecurity threat landscape (European Union Agency for Cybersecurity [ENISA], 2024).

The article concludes that effective regulation should not establish governmental control over "truth". Rather, it should develop risk-based information governance focusing on coordinated manipulative behaviour, algorithmic transparency, content provenance, platform accountability, researcher access to data, media literacy and judicial safeguards. It further argues for progressively integrating information integrity into national cybersecurity frameworks.

Keywords: Cyber Disinformation; Cognitive Sovereignty; Cybersecurity; Information Integrity; Artificial Intelligence; Deepfakes; Digital Platforms; Democratic Security; Information Manipulation.

مقدمة

أحدثت الثورة الرقمية تحولا جوهريا في بنية السلطة داخل المجتمعات المعاصرة؛ إذ لم تعد القوة مرتبطة حصرا بالقدرة على امتلاك الموارد المادية أو المؤسسات السياسية أو وسائل الإعلام التقليدية، وإنما أصبحت القدرة على إنتاج المعلومات وتصنيفها وتوجيهها والتحكم في شروط ظهورها وانتشارها أحد أهم مصادر القوة في العصر الرقمي. ويعني ذلك أن من يملك القدرة على التأثير في تدفقات المعلومات لا يؤثر فقط في ما يعرفه الفرد، وإنما قد يؤثر في الطريقة التي يدرك بها الواقع ويقيم بها المؤسسات والأحداث ويتخذ على أساسها قراراته.

ويكتسب هذا التحول أبعادا غير مسبقة بالنظر إلى الحجم المتزايد للمجال الرقمي العالمي. فقد أفاد الاتحاد الدولي للاتصالات بأن عدد مستخدمي الإنترنت وصل سنة 2025 إلى حوالي 6 مليارات شخص، أي 74% من مجموع سكان العالم، مقابل 5.8 مليارات سنة 2024 ونسبة 71%، مع وجود تفاوت كبير بين الدول مرتفعة الدخل، التي بلغت فيها نسبة الاستخدام حوالي 94%، والدول منخفضة الدخل التي لم تتجاوز فيها النسبة 23% (ITU, 2025). وتكشف هذه المؤشرات أن المجال الرقمي لم يعد فضاءً موازياً للواقع الاجتماعي، وإنما أصبح أحد مكوناته البنوية الأساسية.

غير أن هذا التحول صاحبه ظهور أنماط جديدة من المخاطر لا تستهدف البنية التقنية للأنظمة المعلوماتية حصراً، وإنما تستهدف كذلك المضمون المتداول داخلها والكيفية التي يتشكل بها الإدراك الاجتماعي حوله. وفي مقدمة هذه المخاطر يبرز التضليل السيبراني الذي انتقل من عمليات محدودة لنشر أخبار غير صحيحة إلى منظومات منظمة تستثمر الخوارزميات والحسابات الوهمية وشبكات التنسيق والاستهداف السلوكي والذكاء الاصطناعي التوليدي وتقنيات التزييف العميق.

ولا تتجسد خطورة التضليل المعاصر فقط في إنتاج محتوى غير صحيح؛ إذ قد تقوم العملية التلاعبية على معلومات صحيحة جرى اقتطاعها من سياقها، أو تضخيمها بصورة مصطنعة، أو إعادة توزيعها بواسطة شبكات حسابات تخفي هويتها الحقيقية، أو دمجها بمعلومات مصطنعة في سياق مصمم خصيصاً للتأثير في جمهور معين. لذلك انتقل الاهتمام الدولي تدريجياً من التركيز على «المحتوى الكاذب» إلى دراسة السلوك التلاعب المنظم.

وتبرز هذه النقطة بصورة خاصة في مفهوم التلاعب والتدخل المعلوماتي الأجنبي Foreign Information Manipulation and Interference (FIMI) المستخدم داخل الاتحاد الأوروبي. فوكالة ENISA توضح أن FIMI يشير إلى نمط من السلوك، قد يكون معظمه غير قانوني في ذاته، لكنه يتسم بالطابع المتعمد والمنسق والتلاعب، ويهدد أو يحتمل أن يؤثر سلباً في القيم والإجراءات والعمليات السياسية (ENISA, 2022). ولذلك يختلف المفهوم عن التضليل التقليدي من حيث تركيزه على كيفية تنفيذ العملية وليس فقط على صحة الرسالة أو عدم صحتها.

وتؤكد البيانات الحديثة اتساع نطاق هذه التهديدات. فقد كشف جهاز العمل الخارجي للاتحاد الأوروبي عن رصد أكثر من 500 حادثة FIMI خلال سنة 2024، استخدمت فيها جهات التهديد ما لا يقل عن 25 منصة رقمية و38 ألف حساب، بينما استهدفت العمليات المرصودة 322 منظمة وامتدت إلى 90 دولة (EEAS, 2025). ولا تعكس هذه الأرقام مجرد زيادة كمية في التضليل، وإنما توضح تحوله إلى بنى وشبكات عابرة للمنصات والحدود الوطنية.

ويتزامن هذا التحول مع تغير مفهوم الأمن السيبراني نفسه. فقد كان التحليل التقليدي للأمن المعلوماتي يركز على حماية سرية المعلومات وسلامتها وتوافرها، إلا أن وكالة الاتحاد الأوروبي للأمن السيبراني أصبحت تدرج التلاعب بالمعلومات والتدخل ضمن قائمة التهديدات السيبرانية الرئيسية، إلى جانب البرمجيات الخبيثة وبرامج الفدية والهندسة الاجتماعية والتهديدات الموجهة إلى البيانات وهجمات حجب الخدمة وسلاسل التوريد (ENISA, 2024). ويؤكد هذا التطور أن استهداف الإدراك والثقة والبيئة المعلوماتية أصبح جزءاً من مشهد المخاطر السيبرانية المعاصرة.

وقد أضاف الذكاء الاصطناعي التوليدي بعدا جديدا لهذه الإشكالية، ليس فقط لأنه يسمح بإنتاج صور أو أصوات أو مقاطع فيديو مزيفة، وإنما لأنه يخفض تكلفة إنتاج المحتوى بصورة هائلة، ويمكن من تنويعه وترجمته وتخصيصه واستهداف فئات دقيقة به خلال وقت قصير. ولذلك يشير المشهد الحديث للتهديدات السيبرانية لدى ENISA إلى بروز التضليل المدعوم بالذكاء الاصطناعي والتزييف العميق ضمن الاتجاهات المقلقة في الفضاء السيبراني (ENISA, 2025a).

وقد أصبح هذا التداخل بين الذكاء الاصطناعي والتضليل محلا لتنظيم قانوني مباشر داخل الاتحاد الأوروبي. فالمادة 50 من اللائحة الأوروبية للذكاء الاصطناعي تفرض مجموعة من التزامات الشفافية المرتبطة بالأنظمة التوليدية والمحتوى المصطنع، وأصبحت هذه الالتزامات واجبة التطبيق ابتداء من 2 غشت 2026. وتشمل، من بين أمور أخرى، وضع علامات قابلة للقراءة آليا على المخرجات الاصطناعية، والإفصاح الواضح عن بعض صور التزييف العميق والمحتوى النصي الاصطناعي المتعلق بمسائل المصلحة العامة، وفق الضوابط والاستثناءات التي قررتها اللائحة (European Parliament & Council of the European Union, 2024).

ويثير ذلك سؤالا قانونيا أكثر تعقيدا: كيف يمكن مواجهة التضليل دون تحويل القانون إلى أداة لتحديد الحقيقة أو فرض رواية رسمية؟ فحرية التعبير لا تحمي فقط الآراء الصحيحة أو المقبولة اجتماعيا، وإنما تقوم في أصلها على التعدد والاختلاف وإمكان الخطأ والمراجعة والنقد. ومن ثم فإن التوسع غير المنضبط في تجريم «المعلومات الكاذبة» قد يجعل مكافحة التضليل ذاتها خطرا على الديمقراطية.

وقد أكدت الأمم المتحدة هذا التوازن عندما أطلقت سنة 2024 مبادئها العالمية لنزاهة المعلومات، القائمة على خمسة مرتكزات: الثقة والمرونة المجتمعية، والحوافز السليمة، وتمكين الجمهور، والإعلام المستقل والحر والتعددي، والشفافية والبحث (United Nations, 2024) وهي مقارنة تؤكد أن سلامة البيئة المعلوماتية لا تتحقق عبر الرقابة العامة على المحتوى، وإنما من خلال إصلاح بنية البيئة الرقمية وتمكين المجتمع ورفع مستويات المساءلة.

ومن الناحية العلمية، تنبع أهمية الموضوع من موقعه عند تقاطع عدة فروع قانونية: القانون الدستوري والحقوق والحريات، وقانون الأمن السيبراني، والقانون الجنائي، وقانون حماية البيانات الشخصية، وقانون المنصات الرقمية، وقانون الذكاء الاصطناعي، فضلا عن القواعد المتعلقة بالعمليات الانتخابية والإعلام والاتصال.

أما عمليا، فإن تحول التضليل إلى عمليات منظمة وقابلة للتوسع عبر الذكاء الاصطناعي يفرض على المشرع الانتقال من التدخل اللاحق بعد انتشار المحتوى إلى حوكمة استباقية للمخاطر تشمل المنصات والخوارزميات والإعلانات وأصالة المحتوى والوصول إلى البيانات ومرونة المجتمع.

وبالنسبة للمغرب، تكتسب المسألة أهمية خاصة في ظل الاستراتيجية الوطنية للأمن السيبراني في أفق 2030 التي تؤكد أن التوسع الرقمي غير المتحكم فيه يزيد مساحة الهجوم السيبراني، وأن حماية التحول الرقمي تستلزم تطوير الحوكمة وتعزيز الإطار القانوني والمؤسسي وحماية أنظمة المعلومات الحساسة ورفع القدرة الوطنية على الصمود (Direction Générale de la Sécurité des Systèmes d'Information [DGSSI], 2024).

وتأسيسا على ما سبق، تتمحور الإشكالية المركزية للمقال حول السؤال الآتي:

إلى أي حد أدى تطور التضليل السيبراني والذكاء الاصطناعي التوليدي إلى تحويل نزاهة البيئة المعلوماتية والسيادة الإدراكية إلى مصلحة قانونية جديرة بالحماية، وما الآليات الكفيلة بمواجهة عمليات التلاعب الرقمي دون المساس بحرية التعبير والتعددية والحقوق الأساسية؟

وتتفرع عنها تساؤلات ترتبط بالطبيعة القانونية للتضليل السيبراني، وحدود التمييز بين المحتوى المضلل والسلوك التلاعبي، وعلاقة التضليل بالأمن السيبراني والسيادة، ومدى فعالية النماذج التنظيمية الحديثة، ولا سيما التجربة الأوروبية، وإمكان تطوير مقاربة وطنية منسجمة مع الخصوصيات الدستورية والمؤسساتية المغربية. وللإجابة عن هذه الإشكالية، تعتمد الدراسة المنهج التحليلي لتفكيك أبعاد الظاهرة القانونية والتقنية، والمنهج المقارن لاستقراء النماذج الأوروبية والدولية، إلى جانب الاستناد إلى البيانات الكمية الرسمية المتاحة. وبناء عليه، سيتم تقسيم الموضوع إلى مبحثين:

المبحث الأول: التضليل السيبراني وتحول بنية التهديد من تزييف المعلومة إلى هندسة الإدراك الرقمي.
المبحث الثاني: حكاية التضليل السيبراني وإعادة بناء الاستجابة القانونية القائمة على المخاطر.

المبحث الأول: التضليل السيبراني وتحول بنية التهديد من تزييف المعلومة إلى هندسة الإدراك الرقمي
يكشف تحليل التطورات التقنية الحديثة أن التضليل السيبراني لم يعد مماثلاً للإشاعة أو الدعاية التقليدية. فقد أصبحت عمليات التأثير قادرة على توظيف بنى رقمية معقدة تجمع بين الحسابات غير الأصيلة والاستهداف السلوكي والخوارزميات والإعلانات والذكاء الاصطناعي والأتمتة، بما يسمح بالتأثير المتزامن في أعداد واسعة من المستخدمين. ويقتضي فهم هذه الظاهرة الانتقال من تحليل الرسالة المنفردة إلى تحليل منظومة إنتاجها وتوزيعها وتضخيمها، ثم دراسة الآثار التي يمكن أن تترتب عنها بالنسبة إلى استقلال القرار والثقة المؤسسية والأمن الرقمي.

المطلب الأول: التحول المفاهيمي والتقني للتضليل السيبراني

يطرح التضليل السيبراني صعوبة أولى تتعلق بالتحديد المفاهيمي. فليس كل محتوى غير صحيح تضليلاً، كما أن التضليل لا يستلزم دائماً أن يكون المحتوى نفسه كاذباً بالكامل.

ولهذا أصبح الاتجاه الدولي يميل نحو تبني مفهوم «نزاهة المعلومات» بدلاً من حصر النقاش في «الأخبار الزائفة»، والتركيز على السلوك والوسيلة والبنية والهدف بدلاً من الاقتصر على صحة الجملة محل التداول.

الفقرة الأولى: من الأخبار الزائفة إلى التلاعب المنظم بالبنية المعلوماتية

تميز الدراسات الحديثة بين المعلومات الخاطئة Misinformation التي قد تنتشر دون قصد الخداع، والمعلومات المضللة Disinformation التي تتضمن عنصراً من القصد والتلاعب. غير أن هذا التمييز، على أهميته، لم يعد كافياً لاستيعاب حملات التأثير السيبراني الحديثة.

وقد تبنت منظمة التعاون والتنمية في الميدان الاقتصادي مقاربة أوسع في تقريرها Facts not Fakes الصادر سنة 2024، إذ اعتبرت أن حماية الديمقراطية تقتضي تعزيز نزاهة الفضاء المعلوماتي من خلال ثلاثة محاور مترابطة: رفع شفافية ومساءلة وتعدد مصادر المعلومات؛ تعزيز قدرة المجتمع على مقاومة التضليل؛ وتطوير الحوكمة والمؤسسات العمومية المعنية بحماية نزاهة المجال المعلوماتي. (Organisation for Economic Co-operation and Development [OECD], 2024)

ويكشف هذا التصور عن انتقال مهم من «تنظيم المحتوى» إلى تنظيم البيئة. فمشكلة التضليل قد لا تكمن في المعلومة وحدها، وإنما في الطريقة التي جرى بها تصميم انتشارها؛ إذ يمكن لمجموعة محدودة من الفاعلين استخدام عشرات أو آلاف الحسابات لإنتاج صورة زائفة توهي بأن موقفاً معيناً يحظى بتأييد اجتماعي واسع.

وقد ذهب التعاون بين ENISA وEEAS منذ سنة 2022 في الاتجاه نفسه، حين تم تطوير إطار تحليلي يجمع بين FIMI والأمن السيبراني. ويتميز مفهوم FIMI بتركيزه على السلوك المتعمد والمنسق والتلاعبي بدلاً من الاقتصر على صحة المحتوى (ENISA & EEAS, 2022).

ويكتسي هذا التحول أهمية قانونية عميقة؛ لأن الاعتماد على معيار «الحقيقة والكذب» وحده يمنح الجهة المنظمة سلطة واسعة وخطيرة في تقييم الخطاب. أما التركيز على عناصر موضوعية مثل انتحال الهوية والتنسيق السري والتضخيم المصطنع وإخفاء مصدر التمويل أو إنشاء شبكات غير أصيلة، فإنه يسمح بمواجهة التلاعب دون جعل القانون حكماً عاماً في صحة الأفكار. وتدعم الأرقام الأوروبية هذه القراءة. فوجود أكثر من 500 عملية مرصودة خلال 2024 مرتبطة بنحو 38 ألف حساب عبر 25 منصة على الأقل يعني أن وحدة التحليل لم تعد «المنشور» وإنما الشبكة التي تقف خلفه. (EEAS, 2025) ومن هنا يمكن اقتراح تعريف للتضليل السيبراني باعتباره:

«كل نشاط رقمي متعمد ومنظم يستخدم وسائل أو بنية أو حسابات أو تقنيات رقمية لإنتاج أو تحريف أو إخفاء مصدر أو تضخيم أو تخصيص معلومات بصورة تلاعبية بقصد التأثير غير الشفاف في الإدراك أو السلوك أو الثقة أو القرار». وتتميز هذه الصياغة بأنها تجعل السلوك التلاعبي محور التعريف، بدلا من جعل الدولة مسؤولة عن تقرير حقيقة كل محتوى. الفقرة الثانية: الذكاء الاصطناعي والتزييف العميق وإعادة تشكيل اقتصاد التضليل أدخل الذكاء الاصطناعي التوليدي تحولاً جذرياً في «اقتصاد التضليل»، لأن الخطر لم يعد متعلقاً فقط بجودة المحتوى المصطنع، بل بانخفاض تكاليف إنتاجه وتوسيع نطاقه.

ففي البيئة الإعلامية التقليدية كان إنتاج مقطع صوتي أو مرئي مزيف عالي الجودة يتطلب إمكانيات تقنية ومالية مهمة، أما اليوم فأصبحت نظم الذكاء الاصطناعي قادرة على إنشاء نصوص وصور وأصوات ومقاطع تركيبية بكلفة ووقت أقل بكثير. ويشير تقرير ENISA لعام 2025 إلى أنه حُل 4,875 حادثة سيبرانية خلال الفترة الممتدة من 1 يوليو 2024 إلى 30 يونيو 2025، في بيئة اتسمت بتقارب متزايد بين أنماط التهديدات، وباستخدام الفاعلين الأدوات والتقنيات بصورة متداخلة. كما تواجه الجماهير الأوروبية عمليات FIMI بالتوازي مع أنشطة الجهات المرتبطة بدول والفاعلين الإجراميين والناشطين السيبرانيين. (ENISA, 2025b) ويؤدي الذكاء الاصطناعي في هذا السياق أربع وظائف أساسية.

أولاً، التوليد واسع النطاق؛ إذ يمكن إنتاج عدد كبير من النصوص والصور والمقاطع في مدة قصيرة. ثانياً، التخصيص، بما يسمح بتعديل اللغة والحجج والنبرة وفق خصائص الجمهور. ثالثاً، الترجمة والتوطين، بما يقلص العوائق اللغوية أمام الحملات العابرة للحدود. رابعاً، المحاكاة، حيث يمكن تقليد صورة أو صوت أو أسلوب شخص أو مؤسسة، وهو ما يجعل التزييف العميق أحد أخطر التطبيقات المرتبطة بالتضليل.

وقد استجاب الاتحاد الأوروبي لهذه المخاطر بصورة تشريعية واضحة. فالمادة 50 من قانون الذكاء الاصطناعي الأوروبي تلزم مقدمي الأنظمة التي تولد محتوى صوتياً أو بصرياً أو مرئياً أو نصياً اصطناعياً بضمان إمكانية اكتشاف أن المخرجات منشأة أو معدلة اصطناعياً بواسطة علامات قابلة للقراءة الآلية، ضمن الشروط التي حددها القانون (European Parliament & Council of the European Union, 2024).

كما أوجب القانون في حالات التزييف العميق الإفصاح عن الطبيعة المصطنعة أو المعدلة للمحتوى، مع مراعاة استثناءات و ضمانات مرتبطة بالأعمال الفنية والإبداعية والساخرة وغيرها (European Parliament & Council of the European Union, 2024). وقد أصبحت التزامات المادة 50 مطبقة منذ 2 غشت 2026. (European Commission, 2026a) وفي يونيو 2026 نشرت المفوضية الأوروبية مدونة ممارسة خاصة بوسم وتصنيف المحتوى المنشأ بالذكاء الاصطناعي، دعماً للتطبيق العملي لهذه الالتزامات. (European Commission, 2026b)

ويكشف هذا الاتجاه عن تطور مهم في الفلسفة التنظيمية: فالقانون لا يمنع المحتوى الاصطناعي من حيث الأصل، وإنما يسعى إلى تعزيز شفافية أصله.

ومن هنا يصبح مفهوم Provenance أو «أصالة المصدر وسلسلة المنشأ» محورا محتملا في الجيل المقبل من تشريعات المعلومات؛ إذ لا يحتاج المستخدم دائما إلى جهة تخبره بأن المعلومة صحيحة أو خاطئة بقدر حاجته إلى معرفة: من أنشأها؟ وهل عدلت؟ وهل أنتجها نظام ذكاء اصطناعي؟ وما مصدرها؟

المطلب الثاني: التضليل السيبراني واستهداف السيادة الإدراكية والأمن الرقمي

لا تتوقف آثار التضليل عند تغيير الاعتقاد بشأن واقعة معينة. فالعمليات الأكثر تطورا قد تستهدف إضعاف قدرة المجتمع على تكوين معرفة مشتركة أو الثقة في أي مصدر للمعلومات. ومن هنا يطرح التضليل سؤالاً يتجاوز الأمن السيبراني بمعناه التقني إلى ما يمكن تسميته، لأغراض هذا البحث، السيادة الإدراكية، أي قدرة الفرد والمجتمع والمؤسسات على تشكيل قراراتهم دون خضوع خفي لعمليات تلاعب رقمية منظمة.

الفقرة الأولى: السيادة الإدراكية كامتداد وظيفي للأمن السيبراني

اعتاد القانون الحديث ربط السيادة بالإقليم والسلطة والمؤسسات، ثم أضاف التحول الرقمي مفاهيم مثل السيادة الرقمية وسيادة البيانات. غير أن عمليات التلاعب بالمعلوماتي تفرض التفكير في مستوى ثالث يتعلق باستقلال الإدراك والقرار. ولا يقصد بالسيادة الإدراكية منح الدولة سلطة على أفكار المواطنين؛ بل على العكس، يتعلق المفهوم بحماية الظروف التي تسمح للأفراد بتكوين آرائهم بحرية بعيداً عن عمليات خفية ومنظمة لانتحال الهوية أو تضخيم الرأي أو التلاعب بالمصادر. وتكشف معطيات JEEAS لسنة 2025 أن عمليات FIMI المرصودة خلال 2024 استهدفت 322 منظمة وامتدت إلى 90 دولة، الأمر الذي يوضح مدى تجاوزها للحدود الترابية التقليدية. (EEAS, 2025)

فإذا استطاع فاعل موجود خارج الدولة إنشاء آلاف الحسابات وتوجيه رسائل دقيقة إلى سكانها والتأثير في النقاش حول مؤسساتها، فإن مفهوم الحدود يصبح أقل قدرة على تفسير ممارسة النفوذ.

ويتيح ذلك التمييز بين أربعة مستويات لنزاهة المعلومات:

المستوى التقني: عدم تغيير البيانات أو الأنظمة بصورة غير مشروعة.

المستوى المصدري: إمكانية التحقق من هوية المصدر وأصالة المحتوى.

المستوى الشبكي: عدم تشويه المجال العام من خلال التنسيق السري والحسابات غير الأصلية.

المستوى الإدراكي: حماية استقلال تكوين الرأي والقرار من التأثير الخفي المنظم.

ولا يعني ذلك حماية المواطن من الإقناع أو الدعاية أو الخطاب السياسي؛ إذ إن التأثير جزء طبيعي من الحياة الديمقراطية. وإنما يتعلق الأمر بالفارق بين الإقناع الشفاف والتلاعب الخفي.

ويجد هذا التصور دعماً في مبادئ الأمم المتحدة لنزاهة المعلومات التي تجعل الثقة والمرونة المجتمعية وتمكين الجمهور والشفافية من مرتكزات البيئة المعلوماتية السليمة. (United Nations, 2024)

ومن ثم، فإن السيادة الإدراكية لا تعني «سيادة الدولة على الحقيقة»، وإنما قدرة المجتمع على حماية تعددية الحقيقة من التلاعب المصطنع.

الفقرة الثانية: التضليل كتهديد للأمن الديمقراطي والمؤسسي

تمثل الانتخابات إحدى أكثر البيئات حساسية أمام التضليل السيبراني، لأنها تتعلق بعملية يفترض أن تعكس الإرادة الحرة للناخب. وتعترف التشريعات الأوروبية بهذه المخاطر صراحة. فالمادة 34 من قانون الخدمات الرقمية الأوروبي تلزم المنصات ومحركات البحث الكبرى جداً بتحديد وتحليل وتقييم المخاطر النظامية الناتجة عن تصميم خدماتها وتشغيلها، بما في ذلك الآثار السلبية

الفعلية أو المتوقعة على النقاش المدني والعمليات الانتخابية والأمن العام (European Parliament & Council of the European Union, 2022).

وأصدرت المفوضية الأوروبية سنة 2024 توجيهات خاصة للمنصات الكبرى حول الحد من المخاطر النظامية التي يمكن أن تهدد نزاهة الانتخابات، مع تأكيد ضرورة احترام حرية التعبير والإعلام والتعددية. (European Commission, 2024)

غير أن حصر التضليل في المجال الانتخابي سيكون اختزالاً للمشكلة. فعمليات التلاعب قد تستهدف الصحة العامة والأمن والاقتصاد والسياسة الخارجية والهجرة والكوارث والثقة في المؤسسات.

كما يمكنها أن تتداخل مع هجمات سيبرانية تقنية. فقد أظهر تقرير ENISA لسنة 2024، المستند إلى تحليل أكثر من 11 ألف حادثة وواقعة سيبرانية، أن الإدارة العامة كانت القطاع الأكثر استهدافاً بنسبة 19%، يليها النقل بنسبة 11% والقطاع المالي بنسبة 9%، فيما شكلت هجمات حجب الخدمة وبرامج الفدية أكثر من نصف الأحداث المرصودة. (ENISA, 2024)

ولا يعني ذلك أن كل هذه الحوادث مرتبطة بالتضليل، وإنما يكشف عن بنية تهديدات يمكن أن تلتقي داخلها العمليات التقنية والمعلوماتية.

فيمكن تصور هجوم يبدأ باختراق نظام معلوماتي، يعقبه تسريب انتقائي لوثائق، ثم مزج وثائق حقيقية بمواد مصطنعة، ثم إطلاق شبكة حسابات لتضخيم سردية معينة. وفي مثل هذه الحالة يصبح من الصعب الفصل عملياً بين «الهجوم السيبراني» و«الهجوم المعلوماتي».

ومن هنا يمكن الدفاع عن مفهوم الأمن الرقمي الذي لا يقتصر على حماية صناديق الاقتراع أو أنظمة التصويت، وإنما يشمل حماية نزاهة المجال المعلوماتي الذي يتخذ المواطن داخله قراره.

المبحث الثاني: حكاية التضليل السيبراني وإعادة بناء الاستجابة القانونية القائمة على المخاطر

تكشف المقارنة الدولية عن أزمة واضحة في النماذج التقليدية لمواجهة التضليل. فإذا مُنحت الدولة سلطة واسعة في تحديد «الحقيقة» تعرضت حرية التعبير للخطر، وإذا تُرك التنظيم للمنصات وحدها أصبحت شركات خاصة صاحبة سلطة شبه سيادية على الخطاب العام.

ولهذا بدأت التنظيمات الأكثر تطوراً بالانتقال نحو نموذج ثالث يقوم على إدارة المخاطر والمسؤولية والشفافية والتدقيق، بدلاً من الاعتماد حصراً على الحذف أو التجريم.

المطلب الأول: من رقابة المحتوى إلى المسؤولية النظامية للمنصات والذكاء الاصطناعي

يمثل الاتحاد الأوروبي المثال الأكثر تطوراً على هذا التحول، من خلال الجمع بين قانون الخدمات الرقمية وقانون الذكاء الاصطناعي ومدونات السلوك والإرشادات التنظيمية.

ويكشف هذا النموذج أن المسألة القانونية لم تعد ترتبط فقط بمحتوى المستخدم، وإنما أصبحت تشمل تصميم المنصة والخوارزميات والإعلانات وأنظمة التوصية وآليات توليد المحتوى الاصطناعي.

الفقرة الأولى: قانون الخدمات الرقمية وتكريس منطق المخاطر النظامية

أحدث قانون الخدمات الرقمية الأوروبي تحولاً مهماً في فلسفة تنظيم المنصات. فهو لا يمنح المفوضية سلطة عامة لحذف كل معلومة يعتقد أنها غير صحيحة، بل يفرض التزامات أكبر على المنصات ومحركات البحث ذات التأثير الأوسع.

وتصنف المنصات أو محركات البحث التي تتجاوز 45 مليون مستخدم شهرياً داخل الاتحاد الأوروبي ضمن المنصات أو محركات البحث الكبرى جداً، فتخضع لأشد متطلبات قانون الخدمات الرقمية. (European Commission, 2026c)

وتلزم المادة 34 تلك الجهات بإجراء تقييم دوري للمخاطر النظامية الناشئة عن تصميم الخدمة وتشغيلها واستخداماتها، بما يشمل الأنظمة الخوارزمية. (European Parliament & Council of the European Union, 2022)

أما المادة 35، فتلزمها باتخاذ تدابير معقولة ومتناسبة وفعالة لتخفيف المخاطر، مع أخذ آثار تلك التدابير على الحقوق الأساسية في الاعتبار. وقد تشمل التدابير تعديل تصميم الخدمة ووظائفها وشروط استخدامها وعمليات الإشراف على المحتوى وأنظمة التوصية وغيرها (European Parliament & Council of the European Union, 2022). وتتمثل القيمة القانونية لهذا النموذج في انتقال المسؤولية من السؤال التقليدي:

«هل المنشور غير مشروع؟»

إلى سؤال أوسع:

«هل تصميم المنصة أو نظامها الخوارزمي يولد أو يضخم خطرا نظاميا يمكن توقعه؟»

وهذا التحول بالغ الأهمية بالنسبة إلى التضليل، لأن الضرر قد لا ينتج عن محتوى واحد، وإنما عن التضخيم الخوارزمي والتنسيق المنظم.

وتعزز الاتجاه الأوروبي في 13 فبراير 2025 عندما وافقت المفوضية الأوروبية والمجلس الأوروبي للخدمات الرقمية على دمج مدونة الممارسات المتعلقة بالتضليل داخل إطار قانون الخدمات الرقمية، بما يسمح باستخدامها معيارا للائتمان فيما يتعلق بمخاطر التضليل (European Commission, 2025).

وبذلك انتقل النموذج الأوروبي من التنظيم الذاتي الذي تقوده الشركات بصورة شبه منفردة إلى شكل من التنظيم المشترك الذي يدمج التزامات القطاع الخاص في إطار قانوني ورقابي أوسع.

الفقرة الثانية: قانون الذكاء الاصطناعي وتحول الشفافية إلى التزام قانوني

إذا كان قانون الخدمات الرقمية يهتم بمخاطر المنصات، فإن قانون الذكاء الاصطناعي الأوروبي أضاف طبقة تنظيمية مرتبطة مباشرة بالمحتوى الاصطناعي.

وتنص المادة 50 على التزامات متعددة للشفافية. فيتعين على مقدمي بعض أنظمة الذكاء الاصطناعي التوليدي ضمان أن تكون المخرجات قابلة للكشف بوصفها محتوى جرى توليده أو تعديله اصطناعياً بواسطة صيغة قابلة للقراءة الآلية (European Parliament & Council of the European Union, 2024).

كما يتعين على مستخدمي بعض الأنظمة الإفصاح عن الطبيعة الاصطناعية للمحتوى الذي يشكل تزييفا عميقا وفق الشروط المحددة في القانون، مع قواعد خاصة بالمحتوى الفني والإبداعي والساخر. ويشمل التنظيم أيضا بعض النصوص المنشورة بقصد إعلام الجمهور في مسائل المصلحة العامة ما لم تنطبق الحالات المستثناة قانونا (European Parliament & Council of the European Union, 2024).

وأصبحت هذه الالتزامات واجبة التطبيق في 2 غشت 2026 (European Commission, 2026a).

وتكشف هذه القواعد عن توجه تنظيمي يمكن وصفه بـ«الشفافية قبل الحظر»*. فبدلاً من اعتبار المحتوى الاصطناعي غير مشروع لمجرد أنه اصطناعي، يُلزم الفاعل بالكشف عن طبيعته في السياقات المحددة قانونا.

وهذه المقاربة أكثر اتساقا مع حرية التعبير والابتكار، لأن استخدام الذكاء الاصطناعي في الفن أو التعليم أو البحث أو الترفيه لا يمثل في ذاته تهديدا. والخطر ينشأ حين يُستخدم الاصطناع لإيهام المتلقي بصورة مضللة حول أصالة المحتوى.

ويسمح الجمع بين DSA وقانون الذكاء الاصطناعي ببناء ثلاثية تنظيمية:

مسؤولية المنصة عن المخاطر النظامية؛ ومسؤولية مقدم التكنولوجيا عن قابلية الكشف؛ ومسؤولية المستخدم المهني في الحالات المحددة عن الإفصاح.

وهذه الثلاثية أكثر تقدما من الاختصار على تجريم الشخص الذي يشارك المنشور في نهاية سلسلة معقدة من الإنتاج والتوصية والتضخيم.

المطلب الثاني: نحو نموذج قانوني متعدد المستويات لحماية نزاهة المعلومات والسيادة الإدراكية

لا يعني نجاح بعض عناصر النموذج الأوروبي إمكانية استنساخه حرفيا في جميع الدول، لأن كل نظام قانوني يرتبط بدستوره ومؤسساته وبيئته الإعلامية ومدى استقلال الهيئات الرقابية. لكن المقارنة تسمح باستخلاص مبادئ عامة يمكن أن تشكل أساساً لنموذج متوازن يقوم على حماية نزاهة المجال المعلوماتي دون تأسيس «سلطة للحقيقة».

الفقرة الأولى: مرتكزات النموذج القانوني المتوازن لمواجهة التضليل السيبراني

يقوم المرتكز الأول على التمييز القانوني بين المحتوى والسلوك. فليس كل قول خاطئ عملا غير مشروع، وليس كل معلومة صحيحة بريئة من التلاعب. لذلك يجب أن ينصب اهتمام القانون، بدرجة أكبر، على مؤشرات موضوعية مثل التنسيق الخفي، وانتحال الهوية، والتضخيم الاصطناعي، وإخفاء المصدر، واستخدام شبكات الحسابات غير الأصلية، والتلاعب بالسياق. ويتفق ذلك مع الاتجاه الذي تبنته OECD، والذي يدعو الحكومات إلى التركيز على سلامة النظام المعلوماتي بدل محاولة تنظيم المحتوى بصورة مباشرة (OECD, 2024). أما المرتكز الثاني فهو التناسب.

فلا يجوز أن تكون الاستجابة لمعلومة خاطئة محدودة الانتشار مساوية للاستجابة لعملية منظمة تستهدف الانتخابات أو الصحة العامة أو الأمن. وينبغي بناء سلم للاستجابة يبدأ بالشفافية وتوفير السياق وبيان المصدر، ثم تعطيل التضخيم غير الأصلي، ثم فرض التزامات على المنصة، وصولاً إلى المسؤولية القانونية عندما تتحقق أركان فعل غير مشروع محدد. ويتمثل المرتكز الثالث في المسؤولية النظامية للمنصات.

فالمنصة ليست مجرد قناة صامتة عندما تستخدم نظاما خوارزميا يقرر بصورة نشطة ترتيب المحتوى وتوصيته إلى ملايين المستخدمين. ولذلك ينبغي أن يتناسب مستوى واجباتها مع حجمها وتأثيرها ومخاطرها، على غرار المنطق الذي تبناه DSA. أما المرتكز الرابع فهو شفافية المحتوى الاصطناعي.

وتعد التجربة الأوروبية منذ غشت 2026 نموذجا مهما في هذا الصدد، إذ انتقلت الشفافية من توصية أخلاقية إلى التزام قانوني بالنسبة إلى حالات محددة من المحتوى الاصطناعي والتزييف العميق.

والمرتكز الخامس يتمثل في الوصول العلني إلى البيانات. فلا يمكن تطوير سياسة عمومية رشيدة إذا كانت البيانات المتعلقة بالخوارزميات والانتشار المنسق محصورة لدى الشركات نفسها. ولذلك يجب إيجاد آليات قانونية تسمح للباحثين المؤهلين بالوصول إلى البيانات الضرورية، مع مراعاة حماية الحياة الخاصة والسر التجاري والأمن. ويتمثل المرتكز السادس في ضمانات حقوق الإنسان.

وقد أكدت اليونسكو في مبادئ حوكمة المنصات الرقمية لسنة 2023 أن معالجة التضليل والمعلومات الخاطئة وخطاب الكراهية ينبغي أن تتم مع إبقاء حرية التعبير والحق في الوصول إلى المعلومات في صميم منظومة الحوكمة، وليس باعتبارهما قيودا ثانوية عليها (UNESCO, 2023). وقد اعتمدت هذه الإرشادات بعد عملية مشاور واسعة أنتجت أكثر من 10 آلاف مساهمة من 134 دولة. ويجد المبدأ نفسه سندا في الأمم المتحدة التي دعت الحكومات إلى ضمان التعدد الإعلامي واحترام حرية الرأي والتعبير والامتناع عن التدابير غير المتناسبة مثل عمليات الإغلاق الشامل للإنترنت (United Nations, 2024).

كما يعزز الإطار الاتفاقي الجديد لمجلس أوروبا؛ إذ فتحت الاتفاقية الإطارية بشأن الذكاء الاصطناعي وحقوق الإنسان والديمقراطية وسيادة القانون للتوقيع بتاريخ 5 سبتمبر 2024، وهي أول معاهدة دولية ملزمة قانونيا في هذا المجال، وتهدف إلى ضمان توافق دورة حياة نظم الذكاء الاصطناعي مع حقوق الإنسان والديمقراطية وسيادة القانون (Council of Europe, 2024). ومن هنا يمكن القول إن النموذج القانوني المتوازن لمواجهة التضليل يقوم على قاعدة أساسية:

تنظيم طرق التلاعب أكثر من تنظيم الأفكار، وتنظيم المخاطر أكثر من تنظيم الحقيقة.

الفقرة الثانية: نحو إدماج نزاهة البيئة المعلوماتية في منظومة الأمن السيبراني المغربية

يمتلك المغرب قاعدة مؤسسية وقانونية مهمة يمكن الانطلاق منها لتطوير مقاربة وطنية للتضليل السيبراني، وفي مقدمتها الاستراتيجية الوطنية للأمن السيبراني في أفق 2030.

وتنطلق الاستراتيجية من الاعتراف بأن الرقمنة، رغم فوائدها الاقتصادية والاجتماعية، توسع أيضا مساحة الهجوم وتولد مخاطر يمكن أن تستهدف النظام والأمن العام والاقتصاد والخدمات الحيوية. ولذلك جعلت تطوير الحكامة والإطار القانوني والمؤسسي والاستثمار في الموارد البشرية وحماية أنظمة المعلومات الحساسة وتعزيز المرونة من مرتكزاتها الأساسية (DGSSI, 2024). غير أن تطور طبيعة التهديدات يبرر الانتقال تدريجيا من مفهوم المرونة السيبرانية Cyber Resilience إلى مفهوم أوسع يشمل المرونة المعلوماتية Information Resilience.

ويمكن تعريف الأخيرة بأنها قدرة المجتمع والمؤسسات على اكتشاف واستيعاب ومقاومة عمليات التلاعب بالمعلومات واستعادة الثقة والتدفق الطبيعي للمعلومات دون اللجوء إلى إجراءات تقوض الحقوق والحريات. ويمكن اقتراح ستة محاور لبناء هذا النموذج الوطني.

أولاً: إدماج المخاطر المعلوماتية في تقييم المخاطر السيبرانية الوطنية.

فبدلاً من الاقتصار على الفيروسات والاختراقات وبرامج الفدية، ينبغي تقييم التهديدات الهجينة التي تمزج الهجوم التقني بحملات التأثير.

ثانياً: إنشاء آلية وطنية متعددة الأطراف لرصد نزاهة البيئة المعلوماتية.

ولا ينبغي أن تكون هذه الآلية «هيئة لتحديد الحقيقة»، وإنما فضاء للتنسيق بين الجهات المختصة بالأمن السيبراني والبيانات والاتصال والإعلام والبحث العلمي والجامعات والمجتمع المدني.

ثالثاً: بناء نظام للإنذار المبكر المعلوماتي.

ويمكن أن يركز على الفترات ذات الحساسية المرتفعة، مثل الانتخابات والأزمات والكوارث والهجمات السيبرانية الكبرى، مع اعتماد مؤشرات موضوعية مرتبطة بالشبكات المصطنعة والتضخيم غير الطبيعي وانتحال المؤسسات.

رابعاً: تطوير التزامات الشفافية المتعلقة بالمحتوى الاصطناعي.

وتوفر المادة 50 من القانون الأوروبي للذكاء الاصطناعي تجربة مقارنة مهمة يمكن الاستفادة منها، مع تكييف أي تنظيم وطني مع الدستور المغربي وضمانات حرية التعبير.

خامساً: تقوية التربية الإعلامية والمعلوماتية.

فلا يستطيع القانون حذف كل مادة مضللة من الإنترنت، ولا ينبغي له محاولة ذلك أصلاً. لذلك تمثل القدرة النقدية للمواطن خط الدفاع الأكثر استدامة.

وتؤكد الأمم المتحدة أن تمكين الجمهور أحد المبادئ الخمسة لنزاهة المعلومات، إلى جانب الثقة والمرونة والإعلام التعددي والشفافية والحوافز السليمة (United Nations, 2024).

سادساً: إحداث منظومة للبحث العلمي في التضليل السيبراني.

ف نجاح التنظيم يتطلب بيانات مغربية حول أنماط الاستخدام وانتشار المحتوى المصطنع والسلوك المنسق والتزييف العميق، بدلاً من الاعتماد الكامل على نتائج دراسات أجريت في سياقات أجنبية. ومن المهم في المقابل إحاطة كل هذه الآليات بضمانات دقيقة. فلا ينبغي استخدام مكافحة التضليل لتجريم النقد السياسي أو الآراء غير الشعبية أو الصحافة الاستقصائية أو البحث العلمي أو السخرية. كما يجب أن تخضع القرارات التي تمس المحتوى أو الحسابات أو الحقوق الرقمية لمبادئ الشرعية والضرورة والتناسب وقابلية الطعن والرقابة المستقلة.

ف جوهر السيادة الإدراكية ليس حماية المجتمع من الاختلاف؛ بل حماية حرية الاختلاف نفسها من التلاعب الخفي. وعلى هذا الأساس يمكن صياغة قاعدة قانونية استشرافية على النحو التالي: كلما ازدادت قدرة التكنولوجيا على إخفاء مصدر التأثير وتخصيصه وتوسيعه، وجب أن تزداد في المقابل متطلبات الشفافية وقابلية التدقيق والمساءلة والضمانات القضائية.

خاتمة

أظهر البحث أن التضليل السيبراني يمثل تحولا بنويا في طبيعة المخاطر التي تواجه الدولة والمجتمع في العصر الرقمي. فلم تعد المسألة مرتبطة بمجرد تداول معلومة غير صحيحة، وإنما أصبحت تتصل بالقدرة على تصميم البيئة التي تنتشر فيها المعلومات وتحديد من يراها وبأي ترتيب وتواتر وسياق. وقد عززت ثلاثة تحولات رئيسية هذا التطور.

أولها، التوسع العالمي غير المسبوق للفضاء الرقمي، حيث بلغ عدد مستخدمي الإنترنت ستة مليارات شخص سنة 2025، أي 74% من سكان العالم. (ITU, 2025)

وثانيها، تحول التضليل من منشورات فردية إلى شبكات عمليات منظمة عابرة للمنصات والدول، وهو ما توثقه بيانات EEAS حول أكثر من 500 حادثة خلال سنة 2024، مرتبطة بحوالي 38 ألف حساب عبر 25 منصة على الأقل، واستهدفت 322 منظمة في 90 دولة. (EEAS, 2025)

وثالثها، دخول الذكاء الاصطناعي التوليدي بقوة إلى مجال إنتاج المحتوى، بما يسمح بتخفيض التكلفة وتوسيع الحجم وتخصيص الخطاب ومحاكاة الأشخاص والمؤسسات.

وقد أدى مجموع هذه التطورات إلى تقارب بين الأمن السيبراني والأمن المعلوماتي والأمن الرقمي. ولذلك لم يعد من المستغرب أن تُدرج ENISA التلاعب بالمعلومات والتدخل ضمن مشهد التهديدات السيبرانية إلى جانب التهديدات التقنية التقليدية (ENISA, 2024).

لكن الدراسة خلصت في الوقت ذاته إلى أن مواجهة هذا الخطر عبر تجريم عام وفضفاض لـ«المعلومات الكاذبة» يمكن أن تنتج خطرا موازيا يتمثل في تحويل السلطة العامة إلى مرجع للحقيقة.

ولهذا يمثل الانتقال من تنظيم الحقيقة إلى تنظيم مخاطر التلاعب الخيار الأكثر انسجاماً مع دولة القانون.

وتكشف التجربة الأوروبية هذا التحول بوضوح. فقانون الخدمات الرقمية نقل مركز المسؤولية نحو تقييم المخاطر النظامية ومسؤولية المنصات والخوارزميات، بينما أضاف قانون الذكاء الاصطناعي، ولا سيما المادة 50 التي أصبحت واجبة التطبيق منذ 2 غشت 2026، التزامات مرتبطة بكشف ووسم بعض أشكال المحتوى المصطنع والتزييف العميق (European Parliament & Council of the European Union, 2022, 2024).

كما أظهرت مقاربات الأمم المتحدة و OECD واليونسكو ومجلس أوروبا أن نزاهة المعلومات لا تتحقق بالرقابة وحدها، وإنما تستوجب بيئة تجمع بين الشفافية، والمساءلة، والإعلام الحر، والتربية الإعلامية، والبحث العلمي، والمرونة المجتمعية، وحماية حقوق الإنسان.

وعليه، يمكن استخلاص مجموعة من النتائج المركزية:

1. أن التضييق السيبراني يجب أن يُدرس باعتباره عملية لا مجرد محتوى.
 2. أن السلوك التلاعبي المنسق أكثر ملائمة للتنظيم القانوني من معيار «صحة المعلومة» وحده.
 3. أن الذكاء الاصطناعي جعل شفافية المصدر وأصالة المحتوى من أهم موضوعات القانون الرقمي الحديث.
 4. أن المنصات الكبرى لم تعد وسطاء محايدين بصورة مطلقة، لأن بنيتها الخوارزمية تؤثر في حجم انتشار المحتوى.
 5. أن الأمن السيبراني يتجه تدريجياً إلى تجاوز حماية الأنظمة والبيانات ليشمل حماية نزاهة البيئة المعلوماتية.
 6. أن السيادة الإدراكية يمكن أن تشكل مفهوماً تحليلياً واعداداً في الدراسات القانونية، شريطة فهمها باعتبارها حماية لاستقلال تكوين الرأي وليس سيطرة للدولة عليه.
 7. أن المغرب يمتلك عبر الاستراتيجية الوطنية للأمن السيبراني في أفق 2030 أساساً يمكن تطويره باتجاه إدماج المرونة المعلوماتية إلى جانب المرونة التقنية.
- ويمكن، تأسيساً على ذلك، اقتراح بناء منظومة وطنية لنزاهة البيئة المعلوماتية تقوم على التنسيق بين المؤسسات والجامعات والإعلام والمجتمع المدني والفاعلين الرقميين، مع إقرار أنظمة للإنذار المبكر والبحث والوصول إلى البيانات وشفافية المحتوى الاصطناعي.
- وتظل الضمانة الجوهرية في كل ذلك متمثلة في عدم تحويل مفهوم السيادة الإدراكية إلى «سيادة على الإدراك». فالديمقراطية لا تحتاج إلى مواطنين يتلقون حقيقة رسمية واحدة، وإنما إلى مواطنين قادرين على الاختيار بين مصادر متعددة داخل بيئة لا يجري التلاعب بها خفية.
- وهكذا فإن معركة الأمن السيبراني في السنوات المقبلة لن تتمحور فقط حول السؤال: من يستطيع اختراق النظام؟ بل أيضاً حول سؤال أكثر تعقيداً:

من يستطيع اختراق عملية تكوين الإدراك نفسها؟

وعند هذا الحد يصبح الدفاع عن نزاهة المعلومات امتداداً للدفاع عن سيادة القانون، ويصبح ضمان استقلال الإدراك أحد الأبعاد الجديدة لحماية الإنسان والدولة والديمقراطية في العصر الرقمي.

❖ لائحة المراجع

- Council of Europe. (2024). *Council of Europe Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225)*. <https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence>
- Direction Générale de la Sécurité des Systèmes d'Information. (2024). *Stratégie nationale de cybersécurité à l'horizon 2030*. Administration de la Défense Nationale, Royaume du Maroc. <https://www.dgssi.gov.ma/index.php/fr/publications/strategie-nationale-de-cybersecurite>
- European Commission. (2024). *Commission guidelines for providers of very large online platforms and very large online search engines on the mitigation of systemic risks for electoral processes pursuant to Article 35(3) of Regulation (EU) 2022/2065 (C/2024/3014)*. Official Journal of the European Union. <https://eur-lex.europa.eu/eli/C/2024/3014/oj>
- European Commission. (2025). *The Code of Conduct on Disinformation*. <https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation>

- European Commission. (2026a). *Guidelines on transparency obligations for providers and deployers of certain AI systems*. <https://digital-strategy.ec.europa.eu/en/policies/guidelines-ai-transparency-obligations>
- European Commission. (2026b). *Code of Practice on transparency of AI-generated content*. <https://digital-strategy.ec.europa.eu/en/policies/code-practice-ai-generated-content>
- European Commission. (2026c). *Digital Services Act: Very large online platforms and search engines*. <https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops>
- European External Action Service. (2025). *3rd EEAS report on foreign information manipulation and interference threats*. European Union. <https://www.eeas.europa.eu>
- European Parliament, & Council of the European Union. (2022). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act). *Official Journal of the European Union*, L 277, 1–102. <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>
- European Parliament, & Council of the European Union. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). *Official Journal of the European Union*. <https://eur-lex.europa.eu/eli/reg/2024/1689/oj>
- European Union Agency for Cybersecurity. (2022). *Foreign information manipulation interference (FIMI) and cybersecurity—Threat landscape*. ENISA. <https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape>
- European Union Agency for Cybersecurity. (2024). *ENISA threat landscape 2024*. ENISA. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024>
- European Union Agency for Cybersecurity. (2025a). *Cyber threats*. ENISA. <https://www.enisa.europa.eu/topics/cyber-threats>
- European Union Agency for Cybersecurity. (2025b). *ENISA threat landscape 2025*. ENISA. <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025>
- International Telecommunication Union. (2025). *Facts and figures 2025: Internet use*. ITU. <https://www.itu.int/itu-d/reports/statistics/2025/10/15/ff25-internet-use/>
- Organisation for Economic Co-operation and Development. (2024). *Facts not fakes: Tackling disinformation, strengthening information integrity*. OECD Publishing. <https://doi.org/10.1787/d909ff7a-en>
- United Nations. (2024). *United Nations global principles for information integrity: Recommendations for multi-stakeholder action*. United Nations.
- United Nations Educational, Scientific and Cultural Organization. (2023). *Guidelines for the governance of digital platforms: Safeguarding freedom of expression and access to information through a multi-stakeholder approach*. UNESCO. <https://www.unesco.org/en/articles/guidelines-governance-digital-platforms>