مجلـة البـاحث للـدراسات الأكاديمية
ISSN: 2352-975X ELBAHITH for Academic Studies EISSN: 2588-2368
المجلد: 13 / العدد: 02 / السنة: 2026 /ص ص: 326 - 352

القرين الرقمي بين السيادة المتقاطعة والتوازن المفقود: إشكاليات التنظيم القانوني للنماذج التنبؤية بين متطلبات الأمن القومي وحق الخصوصية

The Digital Twin, Overlapping Sovereignties, and the Lost Balance: Regulatory Dilemmas of Predictive Modeling Between National Security and Privacy

تاريخ الإرسال: 20026/05/25 تاريخ القبول: 2026/03/07

رقية بوقراس* *Roukaia BOUKARRAS*
جامعة مستغانم
University of Mostaganem
مخبر القانون الدستوري والحكم الراشد
Roukai.boukarras@univ-mosta.dz

ملخص:

تستكشف هذه الدراسة الأبعاد الفلسفية والقانونية لمفهوم "القرين الرقمي" باعتباره كياناً معلوماتياً ناشئاً يعيد تشكيل التفاعلات البينية بين الفرد، والمنظومات الأمنية، والبيئة التشريعية. وتأتي هذه المقاربة في ظل واقع يتسم بـ "السيادة المتداخلة" والتنازع الصامت على الصلاحيات بين الدولة الوطنية والشركات التكنولوجية العابرة للحدود والمنصات الرقمية. تنطلق الدراسة من إشكالية محورية تتمثل في مدى إمكانية مأسسة النماذج التنبؤية واستثمارها في تعزيز الأمن القومي دون إلحاق الضرر بجريدتي الخصوصية والكرامة الإنسانية، سعياً نحو صياغة مقاربة توازنية مفقودة في البيئة الرقمية الراهنة.

ولتحقيق هذا المستهدف، تبنت الدراسة منهجاً تحليلياً تأصيلياً يربط بين الأبعاد الفلسفية للقانون ونظرية "الجسد المعلوماتي" من جهة، ومبادئ الشرعية والتناسب الدستورية من جهة أخرى. كما شرّحت الدراسة المخاطر البنيوية المترتبة على معالجة البيانات الضخمة، والتنميط الخوارزمي، والتحول الجذري نحو "الرقابة الاستباقية" للسلوك البشري. وفي شقها التطبيقي، اختبرت الدراسة حدود ومعايير مشروعية توظيف الخوارزميات في الحقلين القضائي والأمني. وخلصت الدراسة إلى تقديم إطار معياري وحوكمي مقترح يوفق بين المتطلبات السيادية للدولة والضمانات الجوهرية لحقوق الإنسان، استناداً إلى ثلاثية: الشفافية

*- المؤلف المُراسل.

الخوارزمية، والمساءلة القانونية، وكفالة الحق في المراجعة البشرية للقرارات المؤتمتة.

الكلمات المفتاحية: القرين الرقمي؛ الجسد المعلوماتي؛ النماذج التنبؤية؛ الحوكمة الخوارزمية؛ حقوق الإنسان الرقمية؛ المساءلة الآلية.

Abstract:

This study explores the philosophical and legal dimensions of the "Digital Twin" concept, conceptualizing it as an emerging informational entity that reshapes the nexus between the individual, security apparatuses, and the legislative environment. This approach is situated within a contemporary reality characterized by "overlapping sovereignties" and a silent jurisdictional tug-of-war between the nation-state, transnational tech conglomerates, and digital platforms. The study addresses a pivotal problematic: the extent to which predictive models can be institutionalized to enhance national security without compromising the core tenets of privacy and human dignity, thereby seeking to restore a lost normative balance. To achieve this objective, the study adopts an analytical-foundational approach that bridges legal philosophy and the theory of the "informational body" with the constitutional principles of legality and proportionality. Furthermore, it dissects the structural risks associated with big data analytics, algorithmic profiling, and the paradigmatic shift toward the preemptive surveillance of human behavior. Lexically and empirically, the study examines the boundaries of algorithmic legitimacy within the judicial and security domains. Ultimately, the study proposes a normative governance framework capable of reconciling the sovereign imperatives of the state with fundamental human rights guarantees, anchored in a threefold paradigm: algorithmic transparency, accountability, and the right to human review of automated decisions.

Keywords: *Digital Twin; Informational Body; Predictive Models; Algorithmic Governance; Digital Human Rights; Automated Accountability.*

مقدمـة:

يشهد العقد الثالث من الألفية الثالثة تحولاً بنيوياً حاداً في القواعد الحاكمة لعلاقة الفرد بمنظومات الأمن والقانون، وهو تحول مدفوع بالقفزات المتسارعة لمنظومات الذكاء الاصطناعي، والخوارزميات الإحصائية، ونماذج التعلم العميق. ولم يعد هذا

التحول الرقمي مجرد جيل جديد من تقنيات الإنتاج أو البنى التحتية المعلوماتية، بل أضحى إعادة صياغة جذرية لجوهر العلاقة الرابطة بين الإنسان والدولة؛ إذ باتت النماذج التنبؤية القائمة على المعالجة الرياضية المتقدمة تمتلك القدرة على استباق السلوك البشري المادي، وتصنيف الأفراد استناداً إلى الجدارة الائتمانية أو الأبعاد الأمنية، وتقييم مستويات خطورتهم الافتراضية قبل الإقدام على أي سلوك مادي ملموس. وفي قلب هذا الفضاء المعقد، يبرز مفهوم "القرين الرقمي" (*Digital Twin*) كظاهرة فقهية وتقنية تتجاوز التوصيف الضيق للبيانات؛ فهو ليس مجرد قاعدة بيانات ساكنة أو أرشيف لمعلومات عابرة، بل هو بنية حسابية ديناميكية تنتج تمثيلاً نسقياً وشاملاً للفرد، يُعتمد عليه كمصدر صلب لاتخاذ قرارات سيادية وإدارية وقضائية تمس مباشرة بالمركز القانوني للشخص الطبيعي وحرياته الأساسية المعترف بها دولياً.

تضع هذه الظاهرة الطارئة الفلسفة القانونية المعاصرة أمام اختبار تشريعي وحقوقي غير مسبوق؛ فمن زاوية تطبيقية، يمكن استثمار هذه النماذج التنبؤية القائمة على الذكاء الاصطناعي في ترقية كفاءة المرفق القضائي، وتعزيز القدرات الاستباقية للأجهزة الأمنية، وصياغة سياسات وقائية قادرة على خفض معدلات الجريمة المنظمة. ولكن على نقيض ذلك، فإن غياب الأطر التشريعية القاطعة والملزمة الحاكمة لاستخدام هذه النماذج الحسابية يؤدي بالضرورة ـ كما بينت العديد من التجارب الدولية المقارنة ـ إلى انحراف هذه الأدوات لتصبح وسائل للتمييز المنهجي الممنهج، والمراقبة الشاملة، وإعادة إنتاج التفاوتات الطبقية والاجتماعية تحت واجهة مضللة من "الموضوعية التقنية". ولا يتوقف هذا الإشكال القانوني عند حدود العلاقة الثنائية الكلاسيكية بين الفرد والسلطة العامة، بل يتعداه ليتشابك مع صعود فاعل ثالث في الساحة الدولية؛ وهي الشركات التقنية الاحتكارية والمنصات الرقمية العابرة

ISSN: 2352-975X ——————————EISSN: 2588-2368

للحدود، التي باتت تفرض "سيادة تقنية" تتقاطع وتتزاحم مع سيادة الدول في التحكم بالبيانات وتوجيه القرارات السيادية المبنية عليها.

ومن هذا المنطلق، تتبلور إشكالية البحث في السؤال المحوري الآتي: إلى **أي مدى يمكن إخضاع ظاهرة "القرين الرقمي" وتطبيقات الذكاء الاصطناعي المرتبطة بها لمنطق القانون والأخلاق، بما يضمن التوازن بين الخصوصية الفردية ومتطلبات الأمن القومي، في ظل فضاء تتوزع فيه السيادة بين الدولة والشركات والمنصات الرقمية العابرة للقارات؟**

تنطلق مقاربة هذه الدراسة من فرضية مركزية مؤداها أن المقاربات التشريعية التقليدية، التي ركزت تاريخياً على حماية "البيانات الجامدة" عبر آليات الموافقة المسبقة وحقوق الوصول والتصحيح، باتت عاجزة وقاصرة عن مواجهة المعالجات الديناميكية المعقدة للنماذج التنبؤية. وتؤسس الدراسة لفرضية أن صياغة توازن حقيقي بين هاجس الأمن وحق الخصوصية تستلزم تفعيل ثلاثة مداخل تشريعية متكاملة: أولاً، إعادة صياغة المفهوم الحقوقي للخصوصية لينتقل من حماية "البيانات الخام" إلى إقرار سيادة الشخص على "نموذجه التنبؤي" المستخلص؛ ثانياً، إخضاع كافة استخدامات الدولة لمنظومات القرين الرقمي لمعايير صارمة من الشرعية والضرورة والتناسب تحت رقابة قضائية فعلية؛ وثالثاً، تجاوز المقاربات التشريعية الوطنية المنفردة نحو بناء حوكمة دولية ترسي حداً أدنى من الحقوق الرقمية الملزمة.

تتبدى فرادة هذه الدراسة وموقعها من الأدبيات الفقهية في كونها لا تقف عند حدود القراءة الوصفية للنصوص أو الخطاب النقدي العام، بل تغوص في عمق الفلسفة القانونية الحاكمة للأنظمة البرمجية المتقدمة، مساهمة في تأصيل "القرين الرقمي" باعتباره امتداداً قانونياً وسيادياً للذات الإنسانية وفكراً حسابياً فاعلاً يعيد هندسة توازن القوى بين المواطن والدولة والسوق. ومن ثم، تسعى الدراسة إلى سد فجوة منهجية واضحة في الفقه المعاصر، متمثلة في الفصل بين كرامة الذات الرقمية

ـ بما تحمله من مفهوم الجسد المعلوماتي وحقوق التفسير ومقاومة التنميط الخوارزمي ـ وبين مقتضيات الأمن الاستراتيجي للدولة في بيئة أصبحت فيها معطيات الذكاء الاصطناعي والتحليل التنبؤي حجر الزاوية في صناعة القرار.

تأسيساً على ذلك، يتجه البحث نحو تحقيق ثلاثة أهداف جوهرية متكاملة جرى توزيعها على ثلاثة محاور رئيسية:

- المحور الأول: التأصيل المفاهيمي والقانوني للقرين الرقمي كبنية حسابية ديناميكية مع ضبط تعريفه إجرائياً لتسهيل المعالجة التشريعية.

- المحور الثاني: التشخيص النقدي لاختلالات التوازن بين المقاربة الأمنية والحقوق الفردية، مع تفكيك مأزق تطبيقي لمبدأي الضرورة والتناسب في البيئة التشغيلية الخوارزمية، وبيان معوقات الرقابة القضائية على أنظمة "الصندوق الأسود" المغلقة.

- المحور الثالث: صياغة نموذج استشرافي متكامل للحوكمة القانونية والرقمية، يعيد هندسة العلاقات بين الفرد والدولة والسوق عبر ترسيخ مبادئ تشغيلية آمرة، وتفعيل هيئات رقابية مستقلة لحماية سيادة الفرد على ملفه الرقمي.

وتكتسب هذه الدراسة راهنيتها بالنظر إلى السياق الدولي الحالي المعبر عن تسارع وتيرة التحولات التشريعية المقارنة، والآثار القضائية الدولية المثارة حول التحيزات المنهجية للنماذج الإحصائية للذكاء الاصطناعي. إنها محاولة لتقديم إضافة نظرية وتطبيقية تسند القضاة والمشرعين وصناع السياسات في فهم هذا التحول العميق، وتعين على صياغة أطر قانونية موضوعية تحمي الإنسان في وجوده المزدوج: المادي والرقمي. ولأجل استيفاء هذه الأبعاد، اعتمد البحث تقسيماً ثلاثي الأبعاد يستجيب لجدلية المعالجة العلمية: المفهوم ـ الممارسة ـ الحل.

ISSN: 2352-975X ——————————EISSN: 2588-2368

المحور الأول: التأصيل المفاهيمي والقانوني للقرين الرقمي في البيئة الرقمية

أولاً: من "الملازمة التراثية" إلى "العملانية الخوارزمية"- التوصيف الأنطولوجي للقرين الرقمي

يستمد مفهوم «القرين» جذوره من الذاكرة الثقافية والدينية العميقة، ولا سيما في السياق الإسلامي، حيث لا يحيل إلى مجرد مصطلح لغوي محايد، بل إلى «بنية وجودية» تلازم الكينونة البشرية؛ ففي المتخيّل العقدي يتجسد القرين في ثنائية ملازمة بين قوى الإرشاد (الملك) وقوى الإغواء (الشيطان). هذه «الملازمة الحتمية» تقدّم مفتاحاً تحليلياً لفهم الطبيعة المتناقضة للقرين الرقمي في عصر منظومات الذكاء الاصطناعي والمنظومات الحسابية المتقدمة؛ فهو كيان خوارزمي ملازم للفرد، يمتلك قدرة مزدوجة على أن يكون أداة «تمكين» تعزّز جودة الحياة والعدالة التنبؤية، أو أن يتحول إلى أداة «استلاب» ومراقبة شاملة إذا ما أُخضِع لمنطق السلطة المطلقة أو الربح الاحتكاري. وقد أشار رودوتا إلى أن حماية المعطيات الشخصية تمثّل وجهاً جديداً لحق الإنسان في حماية ذاته، وأن «الوجود الرقمي» أصبح جزءاً من البنية الأنطولوجية والقانونية للفرد[1].

لغوياً، يحيل مصطلح «القرين» إلى الصاحب الذي لا يفارق، وهو معنى يتطابق بنيوياً مع حالة «الديمومة الرقمية» للأفراد في الفضاء السيبراني؛ حيث يصبح الحضور الرقمي امتداداً مستمراً لوجود الفرد، لا ينقطع بانقضاء الفعل المادي[2]. وفي سياق العلاقات الدولية والسياسات العامة، يكتسب هذا المفهوم دلالة نقدية؛ إذ تُوظَّف الأطر الحسابية المتطورة بوصفها «قريناً سيادياً» يسعى لتمثيل الفرد وتوجيه خياراته عبر خوارزميات التعلم الآلي. وقد أكد تقرير صادر عن مفوضية الأمم المتحدة لحقوق الإنسان أن مجرد إمكانية التقاط بيانات الاتصالات يشكل تدخلاً في الخصوصية، كما أن مجرد وجود برنامج مراقبة جماعية يولّد تأثيراً "مُخدراً" على ممارسة الحقوق الأساسية[3].

يمكن قراءة تشكل القرين الرقمي عبر كرونولوجيا أنطولوجية في أربع مراحل مترابطة:

1- مرحلة التأسيس الرقمي (الأثر السيبراني المشتّت): مع بدايات الإنترنت اقتصر الحضور الرقمي للفرد على «آثار» تقنية بسيطة، في هذا الطور كانت البيانات أشبه برواسب معلوماتية هامشية.

2- مرحلة السياسة الاتصالية (بناء الهوية السيميائية): مع صعود منصات التواصل الاجتماعي تحوّل الفرد إلى «بناء واعٍ» لصورة رقمية عن ذاته، وبدأت ملامح «قرين رمزي» تتشكّل.

3- مرحلة إنترنت الأشياء والبيانات الضخمة (الالتحام الوظيفي): أدى تدفق البيانات من الأجهزة المتصلة إلى تحول القرين إلى «ظلاً بياناتياً» مستمراً، مما أثار إشكالات دولية حول «السيادة على البيانات» العابرة للحدود.

4- مرحلة النمذجة التنبؤية والتحليل الإحصائي المتقدم (السيادة الخوارزمية): لم تعد البيانات الرقمية تقتصر على التوثيق، بل أضحت مادة خام لبناء نماذج الذكاء الاصطناعي التي تستشرف السلوكيات المستقبلية وتقدّر المخاطر، حيث يتخلق «القرين الرقمي» كـ«هوية موازية» مستقلة نسبياً عن الذات الطبيعية.

هذا الاستقلال يتجلى في ثلاثة مستويات حرجة: على مستوى البناء (إذ يُفرَض على الفرد تصور خارجي لهويته)، وعلى مستوى الوظيفة (حيث يُعامَل القرين كمصدر أوثق من التصريحات الذاتية المباشرة)، وعلى مستوى الاستمرارية (حيث يمتد أثر القرين إلى ما بعد تغير سلوك الفرد أو حتى وفاته). بهذا المعنى ينزاح مركز الثقل من «البصمة الرقمية» العابرة إلى «القرين الرقمي» المقيم؛ من الأثر التوثيقي التابع إلى الامتداد الأنطولوجي الذي يشارك فعلياً في تشكيل المصير الحقوقي والسياسي للإنسان.

ISSN: 2352-975X ——————————EISSN: 2588-2368

ثانياً: من ملكية البيانات إلى "الجسد المعلوماتي"- التكييف القانوني للقرين الرقمي

أمام هذا التحول الأنطولوجي، يجد الفكر القانوني نفسه مضطراً إلى مراجعة عميقة للمنظور الكلاسيكي الذي تعامل مع البيانات الشخصية كـ«أصول معلوماتية» قابلة للبيع والترخيص والتنازل. هذا التصور يغدو قاصراً حين يتعلق الأمر بالقرين الرقمي بوصفه بنية بياناتية- خوارزمية تعيد تركيب صورة الشخص القانونية في الفضاء السيبراني بفعل آليات المعالجة المؤتمتة.

الاتجاهات الفقهية الحديثة- وفي مقدمتها المدرسة الحقوقية التي يمثلها ستيفانو رودوتا- تذهب نحو اعتبار البيانات الشخصية جزءاً من «الهوية الجسدية الموسّعة» للفرد؛ أي أن المساس غير المشروع بالبنى البياناتية التي تشكّل القرين الرقمي هو مساس بالكرامة الإنسانية، لا مجرد اعتداء على ملكية مادية أو معنوية عابرة[4]. وقد أكدت لجنة حقوق الإنسان التابعة للأمم المتحدة في تعليقها العام رقم 16 أن جمع وحفظ المعلومات الشخصية بواسطة المنظومات التقنية يجب أن ينظمه القانون بوضوح[5]. كما أشار تقرير أممي إلى أن تجميع البيانات التعريفية ("*metadata*") عبر خوارزميات التنميط قد يكشف أنماطاً سلوكية وعلاقات اجتماعية تتجاوز محتوى الاتصالات نفسها. بهذا المعنى يغدو الحديث عن الحقوق التقليدية في «ملكية البيانات» قاصراً وقاصراً جداً في توفير الحماية اللازمة.

يقود هذا الانزياح الفقهي إلى نتيجتين جوهريتين:

1- عدم جواز التنازل الكلي عن السيطرة على القرين الرقمي لأنه يمس جوانب من الكرامة غير القابلة للتفويت البشري.

2- ضرورة الانتقال الحاسم من حماية «موضوع خارجي» إلى حماية «ذات ممتدّة» تفرض سيادتها على امتدادها السيبراني. على هذا الأساس، يكتسب القرين الرقمي المشكل عبر تقنيات الذكاء الاصطناعي «شبه شخصية قانونية» تنتج آثاراً قانونية مباشرة وعميقة (كرفض تأشيرة، أو حرمان من ائتمان، أو حتى تصنيف أمني

استباقي). وقد نصت المبادئ الدولية لتطبيق حقوق الإنسان على مراقبة الاتصالات (2014) على أن المراقبة الخوارزمية يجب ألا تُستخدم إلا كإجراء استثنائي، شريطة أن تخضع لشروط صارمة من الشرعية والضرورة والتناسب والإذن القضائي المسبق(6).

وفي إطار القانون الدولي العام، يمكن تفكيك العناصر البنيوية المشكلة للقرين الرقمي من خلال أربع طبقات رئيسية متكاملة: البيانات السيادية الأساسية (التي تشمل الهوية القانونية والخصائص البيومترية)، السجل السلوكي الديناميكي (الذي يرصد التفاعلات الرقمية المستمرة والتنميط الخوارزمي)، الهوية العلاقية والشبكية (التي ترسم الخرائط الاجتماعية والروابط التفاعلية)، وأخيراً السلوك الزمني والاستجابة اللحظية (التي تقيس المؤشرات الزمنية الدقيقة وردود الأفعال اللحظية). ومن خلال هذه البنية المركّبة، يغدو القرين الرقمي «جسداً معلوماتياً» حقيقياً يمثّل امتداداً نفسياً وعضوياً للشخصية الإنسانية في الفضاء السيبراني المعاصر.

ثالثاً: نحو تعريف إجرائي للقرين الرقمي كامتداد قانوني للذات البشرية

إن التعقيد الأنطولوجي والقانوني المتشابك للقرين الرقمي يفرض قطعاً منهجياً مع الرؤية الكلاسيكية التي عاملت البيانات الشخصية كـ«محتوى جامد» يمكن تملّكه أو التفويت فيه، لصالح مقاربة فقهية حديثة ترى أننا أمام «امتداد معلوماتي أصيل للشخصية الإنسانية» لا يمكن فصله عنها. لذلك، لا يمكن الاكتفاء بالتوصيف التقني البحت للقرين الذي تقدمه هندسة البرمجيات؛ بل ينبغي إسناده مباشرة إلى مكانه الجوهري في البنية الحقوقية والسياسية المعاصرة.

انطلاقاً من هذا الأفق الفلسفي والتشريعي، يمكن اقتراح تعريف إجرائي جامع ومنضبط للقرين الرقمي على النحو الآتي:

ISSN: 2352-975X ——————————EISSN: 2588-2368

القرين الرقمي هو بنية بياناتية- خوارزمية دينامية، تُنشأ عبر تجميع ومعالجة متواصلة لمختلف البيانات المتصلة بشخص طبيعي بواسطة أنظمة الذكاء الاصطناعي، وتُستخدم لتمثيله رقمياً والتنبؤ بسلوكه وإنتاج آثار قانونية أو عملية مباشرة بشأنه، بما يجعل منه امتداداً معلوماتياً صلباً للشخصية الإنسانية يخضع بالضرورة لحماية حقوق الإنسان وقواعد الشرعية وسيادة القانون.

يتضمن هذا التعريف الإجرائي المقترح أربعة عناصر جوهرية متداخلة: البنية الديناميكية (التي تميز القرين عن الملفات الإحصائية الساكنة)، المعالجة المتواصلة متعددة الأبعاد (التي تدمج الأبعاد الأربعة للبيانات بصفة مستدامة)، التمثيل وإنتاج الآثار (الذي يربط مخرجات النموذج بالمسؤوليات الإجرائية والقرارات الإدارية)، والامتداد الحقوقي للشخصية (الذي يدرج هذا الكيان الحسابي ضمن منطق الكرامة الإنسانية وحق الخصوصية الصارم).

رابعاً: سياقات التوظيف السيادي للقرين الرقمي

يتجاوز استغلال القرين الرقمي الأطر التجارية وحسابات السوق الائتمانية ليتغلغل في صميم الوظائف السيادية والرقابية للدولة. ففي سياقات الأمن التنبؤي وتطبيقات الذكاء الاصطناعي الشرطي، يُستخدم هذا القرين لرصد «مسارات الخطر» وتقييم احتمالات الجنوح قبل وقوع الفعل المادي، فيتحول القرين الخوارزمي إلى محور ترتكز عليه العلاقة البنيوية الجديدة بين المواطن والسلطة العامة[34]. كما يُستثمر على نطاق واسع في بناء قواعد بيانات سيادية ضخمة تمنح الأجهزة التنفيذية رؤية بانوبتية شاملة، في حين تسمح تقنيات الاستهداف الجزئي وتوجيه الرأي العام بتخصيص الرسائل السياسية والانتخابية لكل فرد بدقة متناهية وفقاً لخصائص قرينه الرقمي المشكّل خوارزمياً، مما يفتح الباب على مصراعيه أمام أشكال غير مسبوقة من «هندسة الوعي الجمعي» وتوجيه الإرادة الشعبية.

وفي فضاء تداخل هذه الاستخدامات، يبرز القرين الرقمي كمساحة توتر حاد ونزاع قيمي بين مستوى الكرامة الفردية والحرية الشخصية، ومستوى الأمن القومي ومقتضيات الاستقرار الاستراتيجي للدولة (والذي يفرض إخضاع هذه الممارسات لمعايير الشرعية والضرورة والتناسب الدولية)، ومستوى السيادة الرقمية الدولية وتنازع القوانين عابر الحدود. هذا التشابك المعقد يبيّن بصورة قاطعة أننا لا نواجه مجرد تطور تقني أو برمجيات عابرة، بل نحن أمام إعادة صياغة جذرية لعلاقة الإنسان بآليات السلطة والنفوذ في الفضاء السيبراني، وهو ما يمهّد الطريق منطقياً للانتقال نحو تفكيك هذه الممارسات في المحور الثاني.

المحور الثاني: جدلية الأمن والحرية في ظل المراقبة الرقمية والخوارزمية

إذا كان المحور الأول قد انتهى إلى تأصيل "القرين الرقمي" باعتباره امتداداً وجودياً وحقوقياً للذات الإنسانية في الفضاء الافتراضي، فإن هذا المحور يتقدم خطوة أبعد لتفكيك الكيفية التي يتحول بها هذا الامتداد إلى حيز صراعي تتقاطع وتتواجه داخله الدولة ـ بمنطق استدامة الأمن القومي ـ والفرد البشري ـ بمنطق صيانة الحرية وحقوق الإنسان. إننا نقف هنا أمام تحول بنيوي في فلسفة العقيدة الأمنية المعاصرة؛ إذ انزاح الثقل من مفهوم الرقابة اللاحقة على الجريمة والحدث المادي إلى نموذج "الأمن الاستباقي" القائم على معالجة كتل البيانات الضخمة ونماذج الذكاء الاصطناعي التنبؤية، وهو ما يعيد طرح سؤال العقد الاجتماعي على قاعدة فلسفية جديدة: فلا مواطنة حقيقية اليوم بلا حضور رقمي فاعل، ولا سيادة وطنية فعليّة بلا سيطرة وإشراف على تدفقات البيانات المستخلصة من حركة المجتمع. وبين سلطة عامة ترى في بناء القرين الرقمي ضمانة محورية للاستقرار والاستشراف الوقائي، وفرد طبيعي يخشى من تحول هذا الامتداد المعلوماتي إلى "سجّان خوارزمي"، تتبلور الجدلية الحادة والعميقة بين ضرورات الأمن ومتطلبات الحرية.

ISSN: 2352-975X ——————————EISSN: 2588-2368

أولاً- توظيف القرين الرقمي كمورد استراتيجي للأمن القومي (الاستباق والرقابة الوقائية)

1- الأمن التنبؤي وتحويل القرين الرقمي إلى استخبار وقائي: شهدت الممارسات الأمنية لإنفاذ القانون في العقدين الأخيرين انخراطاً مكثفاً في ما يمكن تسميته بـ"زمن الاستباق الخوارزمي"، فلم يعد الهدف التشغيلي مقتصراً على إجراء التحريات والتحقيقات الجنائية التقليدية عقب وقوع الفعل المادي للجريمة، بل أصبح الرهان الاستراتيجي منصبّاً على كبح الجريمة وإجهاضها في مهدها الافتراضي قبل أن تتحول إلى سلوك مادي ملموس. وهنا يتجلى مفهوم "الأمن التنبؤي" القائم على تطويع خوارزميات الذكاء الاصطناعي لتحليل كتل البيانات الضخمة المتولدة عن الأقران الرقمية للأفراد، سعياً وراء رصد أنماط سلوكية معينة تُقرأ خوارزمياً كمؤشرات مبكرة على الجنوح أو الانحراف الإجرامي. وفي هذا السياق التنفيذي، لا يُنظر إلى القرين الرقمي بوصفه مجرد أثر تقني عابر أو نتاج جانبي لاستخدام الشبكات، بل يتم التعامل معه كمنجم معلوماتي سيادي يستبطن أدق تفاصيل الفرد، وعاداته، وشبكات علاقاته، وميوله الفكرية والسلوكية. وقد كشفت الدراسات والتقارير الحقوقية المعاصرة أن أنظمة الرصد الحسابية المعتمدة في إنفاذ القانون تعاني من تحيزات إحصائية عرقية وإثنية موثقة، حيث أظهر نظام *COMPAS* المستخدم في تقييم خطر العود الإجرامي وتحديد الأحكام الجنائية تحيزاً منهجياً كبيراً وضاراً بحقوق الأقليات(7).

وعليه، تتغير طبيعة العمل الاستخباري والأمني لتتحول من منطق "رد الفعل" الشرطي إلى منطق "الفعل الوقائي المستدام"، حيث يصبح القرين الرقمي هو الموضوع الأساسي للرقابة والتحليل الدائمين عوضاً عن الجسد المادي للمواطن. وتتبدى خطورة هذا الانزياح الفلسفي في اعتماده المطلق على منطق "الارتباط الإحصائي" (*Correlation*) على حساب منطق "السببية القانونية"

(*Causation*)؛ فمجرد وجود تشابه نمطي في السمات الرقمية بين قرين فرد عادي وقرين شخص آخر صُنِّف مسبقاً كـ "مصدر خطر" قد يكون مسوّغاً كافياً لوضع المواطن الأول تحت طائلة رقابة لصيقة وإجراءات احترازية مقيدة. هنا ينشأ مفهوم "العقاب الرقمي القبلي"، وهو نوع من العقوبة المقنعة التي لا تتأسس على فعل مادي جرى ارتكابه، بل على ما "يُحتمل أن يُفعل" مستقبلاً بناءً على استنتاج إحصائي افتراضي. ويترافق هذا المنحى مع خطاب سياسي يقدّم "الشفافية الرقمية الشاملة" كثمن ضروري ولا بديل عنه لاستدامة الاستقرار، وهي معادلة تضع الحق الأصيل في الخصوصية وحماية البيانات في مواجهة صعبة ومباشرة مع دواعي الضرورة الأمنية للدولة.

2- بناء قواعد البيانات السيادية وهندسة السلوك الجمعي: لا يتوقف التوظيف الاستراتيجي للقرين الرقمي عند حدود التتبع الفردي أو الرصد الجنائي المقيد، بل يتجاوزه ليدخل في هندسة ما يُعرف بـ "قواعد البيانات السيادية الضخمة"؛ وهي مستودعات بيانات وطنية تدمج السجلات المدنية، والمالية، والصحية، والسلوكية، والاتصالية لتشكيل مرآة رقمية كلية ومحدثة باستمرار عن المجتمع ككل. إن حيازة الدولة لقرين رقمي مفصل لكل مواطن يمنح الأجهزة التنفيذية قدرة غير مسبوقة على قراءة البنية النفسية والاجتماعية للكتلة البشرية، واستشراف اتجاهات الرأي العام، وتحديد بؤر الاحتقان الاجتماعي بدقة متناهية.

وفي فترات الأزمات الوطنية أو الاستحقاقات السياسية الكبرى، يمكن لهذه الأقران الرقمية المجمعة أن تتحول من أدوات رصد ساكنة إلى قنوات بالغة الدقة لهندسة وتوجيه السلوك الجمعي. فمن خلال توظيف تقنيات "الاستهداف الجزئي" (*Micro-targeting*) التي تتيحها برمجيات الذكاء الاصطناعي، يغدو بمقدور صناع القرار وصناع الحملات توجيه رسائل اتصالية مبطنة ومصممة خصيصاً لكل شريحة مجتمعية بناءً على نقاط الضعف والميول المستخلصة من دراسة قرينهم الرقمي. بيد أن

ISSN: 2352-975X ——————————EISSN: 2588-2368

هذه القدرة التوجيهية الهائلة تثير إشكالات أخلاقية وقانونية عميقة في فقه القانون العام: فأين تنتهي حدود الاتصال العمومي التوعوي المشروع للدولة، وأين تبدأ عمليات التلاعب النفسي وهندسة الرأي العام التي تمس في الصميم كرامة الإرادة السياسية وحرية الاختيار الديمقراطي؟

وفي هذا الفضاء المتشابك، تتبلور "السيادة الرقمية" كقدرة حصرية للدولة على بسط رقابتها القانونية على تدفقات البيانات، وفرض مبدأ توطينها داخل الحدود الوطنية. فالدولة التي تعجز عن فرض سيادتها التشغيلية على الأقران الرقمية لمواطنيها تظل مكشوفة أمنياً واستراتيجياً أمام تغول الشركات التكنولوجية الكبرى العابرة للقارات. ومن هنا، تصاعدت وتيرة السياسات التشريعية الرامية إلى توطين البيانات واعتبارها مورداً سيادياً غير قابل للاستباحة، مما خلق حالة من التوتر المزدوج والمستمر: بين الدولة والشركات الرقمية الاحتكارية من جهة، وبين الدولة والمواطن من جهة أخرى، والذي يرى تفاصيل حياته وقرينه الافتراضي يتحولان إلى مادة خام تتنازع السيطرة عليها قوى السيادة والسوق.

ثانياً- ضمانات سيادة القانون في مواجهة تغوّل "الدولة الأمنية الرقمية"

1- مأزق "الضرورة والتناسب" في الرقابة الخوارزمية: إن المبدأ الدستوري المستقر الذي يجعل من "الحرية" أصلاً ومن "التقييد" استثناءً يتعرض لاختبار قاسي وفشل وظيفي في البيئة التشغيلية الرقمية، حيث يتم التوسع في تفسير "حالة الاستثناء" لتبرير رقابة شاملة ومستمرة تفقد الحقوق جوهرها. وقد تواترت تقارير مفوضية الأمم المتحدة لحقوق الإنسان لتؤكد أن أي تدخل في الحق في الخصوصية لا يمكن وصفه بالمشروعية إلا إذا كان منصوصاً عليه صراحة بموجب قانون واضح ومتاح، وموجهاً لتحقيق هدف مشروع ومحدد، ومستوفياً بصرامة لاختباري الضرورة والتناسب الحقوقيين[8]. كما شددت تقارير المقرر الخاص المعني بالحق في الخصوصية على ضرورة تضييق تبريرات "الأمن القومي" بحيث تقتصر حصراً على

الحالات المهددة لكيان الأمة ووجودها، دون اتخاذها غطاءً لانتهاك الحريات الفردية[9].

بيد أن تطبيق معيار "التناسب" بالمعنى الرقمي واجه مأزقاً فنياً وفقهياً؛ فجمع معلومة بسيطة أو بيان قد يبدو تافهاً في حد ذاته، يمكن عند معالجته ودمجه عبر خوارزميات الذكاء الاصطناعي والتعلم الآلي أن يتحول إلى نموذج تنبؤي شديد الدقة والعمق يخترق أخص خصوصيات الفرد وحياته الحميمة. بناءً على هذا الواقع، لم يعد كافياً في المنظور الفقهي الحديث الاكتفاء بحماية "البيان المفرد" أو المعطى الشخصي الخام، بل أصبح من الواجب الدستوري بسط الحماية القانونية على "النموذج التحليلي الكلي" الناتج عن عمليات الاستنتاج والتنميط الآلي التي تجريها الأنظمة الحسابية.[10]

2- الرقابة القضائية المستقلة وشفافية "الصندوق الأسود": تظل الرقابة القضائية المستقلة والمسبقة هي خط الدفاع الدستوري الأخير لصيانة الحقوق، غير أن القضاء التقليدي يواجه عجزاً معرفياً وتحديات تقنية بالغة التعقيد أمام الطبيعة المصمتة للخوارزميات التي تنتج قرارات تمس المراكز القانونية للأفراد. وقد فجرت القضية الشهيرة *Loomis v. Wisconsin (2016)* نقاشاً دستورياً وقانونياً واسعاً حول مدى مشروعية اعتماد المحاكم على خوارزميات سرية لا تلبي معايير المحاكمة العادلة وحق الدفاع[11]. ففي هذه القضية، استندت المحكمة إلى نظام *COMPAS* الحسابي لتقييم خطورة المتهم وفرص إعادة إدماجه، لكن الشركة التجارية المطورة للنظام تمسكت برفض الكشف عن آلية عمل الخوارزمية والمعايير الحسابية المعتمدة، متذرعة بحماية أسرارها التجارية وحقوق ملكيتها الفكرية، مما وضع العدالة في مواجهة قرار مصمت لا يمكن مراقبته أو الطعن فيه[12].

ولتجاوز هذا المأزق الإجرائي، تبرز حاجة ملحة لتطوير منظومة "القضاء المتخصص" ودعم الهيئات القضائية بمختبرات خبرة تقنية مستقلة قادرة على تفكيك

ISSN: 2352-975X ——————————EISSN: 2588-2368

الشيفرات البرمجية. وفي هذا الصدد، خطا المشرع الأوروبي خطوة متقدمة عبر اللائحة العامة لحماية البيانات (*GDPR*)، حيث أقر للأفراد حقاً صارماً في عدم الخضوع لقرارات مؤتمتة بالكامل تنتج آثاراً قانونية بحقهم، مع كفالة "الحق في التفسير" (*Right to Explanation*) لمعرفة المنطق الحسابي الذي بني عليه القرار[13]. وتأكيداً على هذا المنحى الإجرائي، أصدرت الهيئة الهولندية لحماية البيانات في أبريل 2026 إرشادات توجيهية ملزمة تفصّل الشروط الفنية لاعتبار التفسير الخوارزمي قانونياً ومفهوماً للشخص الطبيعي[14]. وتناغماً مع هذا الاتجاه، أكدت محكمة العدل الأوروبية أن نيل "معلومات ذات دلالة حول المنطق الرياضي الكامن" خلف القرار الآلي يجب أن يُفسر بروح موسعة تضمن للفرد استيعاب القرار والتحقق من سلامته[15].

3- نحو ميثاق لحقوق "الإنسان الرقمي": إن هذه الجدلية العميقة تطرح سؤالاً فلسفياً وقانونياً يتجاوز الأطر التشريعية القائمة: فهل يعقل أن تتجند القوانين لحماية الجسد المادي للإنسان وحريته في التنقل، بينما تترك امتداده الوجودي المتمثل في "قرينه الرقمي" مستباحاً لبناء النماذج والتلاعب الخوارزمي دون حماية؟ من هنا، تنبري الاتجاهات الفقهية المعاصرة للمطالبة بصياغة "ميثاق عالمي لحقوق الإنسان الرقمي"، يؤصل لمجموعة من الحقوق اللصيقة بالشخصية الرقمية؛ وفي مقدمتها الحق في استخدام التشفير القوي كأداة حماية ذاتية، والحق في رفض التنميط الخوارزمي الشامل، والحق في السيادة الكاملة على الملف الرقمي، فضلاً عن فرض مبدأ الشفافية الجبرية على كل معالجة آلية تتناول البيانات البشرية.

ثالثاً- بين هاجس الأمن وشغف الحرية: توازن العقد الرقمي

إن إفراط الأنظمة السياسية في تغليب هاجس الأمن والاستقرار إلى حد ابتلاع القرين الرقمي وإلغاء القيود التشريعية، يقود بالضرورة إلى إعادة إنتاج نموذج "الدولة البانوبتية" الشاملة التي تمحي فيها الحدود الفاصلة بين الفضاء العام والحياة

الخاصة للأفراد. وقد جاءت "المبادئ الدولية لتطبيق حقوق الإنسان على مراقبة الاتصالات (2014)" لتؤكد كنص مرجعي أن أي تدخل تقني في الحياة الخاصة لا بد أن يظل تدبيراً استثنائياً محاطاً بضمانات قضائية صارمة ومحكوماً بضرورة اجتماعية ملحة[16]. إن الرهان الحقيقي الذي يعالجه هذا المحور هو البحث عن صيغة متوازنة لعقد اجتماعي رقمي جديد؛ صيغة تعترف للدولة بسلطتها المشروعة في صيانة الأمن واستباق المخاطر، لكنها تقيد هذه السلطة بضوابط الشرعية، والتناسب، والرقابة القضائية الناجزة، بما يحول دون تحول التقنية من أداة لخدمة الإنسان إلى وسيلة لإلغاء وجوده الحقوقي.

المحور الثالث: آفاق التعايش بين القرين الرقمي وحقوق الإنسان- نحو عقد اجتماعي رقمي وحوكمة أخلاقية للمنظومات الحسابية

يأتي هذا المحور بمثابة انتقال منهجي حاسم من مرحلة التشخيص والتفكيك النقدي (التي استغرقها المحوران الأول والثاني) إلى أفق الاستشراف وبناء البدائل القانونية؛ فإذا كان القرين الرقمي قد غدا امتداداً وجودياً وحقوقياً لا ينفصم عن الذات البشرية، وإذا كانت عقيدة الدولة الأمنية المعاصرة قد اندفعت نحو تبني ممارسات المراقبة الخوارزمية على نحو أربك التوازن الدستوري بين مقتضيات الأمن وحرمة الحرية، فإن السؤال المصيري الذي يواجه الفقه التشريعي يتلخص في: كيف يمكن صياغة نمط تعايش مؤسسي يضمن استدامة الأمن دون سحق الحقوق الأساسية، ويستثمر معطيات الطفرة التقنية دون تحويلها إلى أدوات للهيمنة والاستلاب؟ إن الإجابة الفقهية الرشيدة لا تكمن في الرفض الانكفائي للتقنية، ولا في إطلاق عنانها بلا ضوابط كابحة، بل تتجسد في صياغة "عقد اجتماعي رقمي جديد" يعيد هندسة توازن القوى وتوزيع الصلاحيات بين الدولة، والفرد، وقوى السوق المحتكرة.

ISSN: 2352-975X ——————————EISSN: 2588-2368

أولاً: من "سلطة البيانات" إلى "حكم القانون الرقمي"

إن أحد أخطر الانزياحات البنيوية التي واكبت العصر الرقمي تتمثل في انتقال مركز السلطة والتحكم من النص القانوني الكلاسيكي إلى هندسة المنظومات البرمجية ذاتها؛ إذ لم تعد الخوارزميات مجرد أدوات تقنية "تطبّق" إرادة المشرع، بل تحولت في كثير من الأحيان إلى جهات تنتج قواعد سلوكية فعلية وتفرضها كأمر واقع. وبناءً عليه، يغدو التحدي المركزي أمام فقه القانون العام هو إخضاع هذه الرقمنة لسيادة القانون وتحويلها من سلطة واقع تقني مجرد إلى بنية قانونية محكومة بالشرعية. ويتطلب هذا التحول إرساء مبدأ دستوري جازم يقضي بعدم جواز اتخاذ أي قرار يمس بالحقوق اللصيقة بالشخصية أو الحريات العامة دون استناده إلى أساس تشريعي واضح ومسبق، ودون كفالة مسارات مراجعة مستقلة، وإتاحة تفسير بشري عقلاني وقابل للفهم الفقهي والقانوني.

ثانياً: مبادئ حاكمة لتصميم واستخدام الأنظمة الخوارزمية في المجال العام

إن السيطرة القانونية على تداعيات القرين الرقمي تستلزم بلورة جملة من المبادئ المعيارية الآمرة التي يمكن ترجمتها إلى سياسات تشريعية تطبيقية. وتستلزم هذه الصياغة الانطلاق من الأطر التنظيمية الدولية القائمة والمتمثلة في: اللائحة العامة لحماية البيانات الأوروبية *GDPR*)، والتشريعات الأوروبية الحديثة المنظمة لتقنيات الذكاء الاصطناعي، فضلاً عن توصية اليونسكو بشأن أخلاقيات التقنيات المؤتمتة ومخرجاتها:

1- الشرعية وتحديد الغرض: تفرض القواعد التشريعية ربط كل عملية معالجة للبيانات الشخصية بغرض مشروع، ومحدد، ومعلن سلفاً، مع حظر ما يُعرف بـ "الزحف الوظيفي" للمنظومات الأمنيّة. وتأسيساً على هذا المنحى، أوجبت المادة 5(1)(ب) من اللائحة العامة لحماية البيانات (*GDPR*) أن تكون الغايات الكامنة وراء المعالجة "محددة، وصريحة، ومشروعة"[17].

EISSN: 2588-2368 ——— ISSN: 2352-975X

2- الضرورة والتناسب وتقليل البيانات: يستوجب إعداد الأنظمة التنبؤية تفعيل مبدأ "الحد الأدنى من المعطيات" المنصوص عليه في المادة 5(1)(ج) من اللائحة الأوروبية، بحيث يقتصر الجمع على ما هو ضروري حتماً لتحقيق الغاية[18]. وقد جاءت المبادئ الدولية لتطبيق حقوق الإنسان على مراقبة الاتصالات (2014) لتؤكد أن أي تدبير تقني يمس الخصوصية يجب أن يكون "محدداً بدقة ومتناسباً مع الهدف المشروع"[19] .

3- العدالة وعدم التمييز الحسابي: يحظر الفقه التشريعي الحديث كافة منظومات "التنميط الاجتماعي" وأدوات "الشرطة التنبؤية" التي تتأسس بنيتها على التمييز الخوارزمي الآلي. ويستند هذا الحظر إلى ما كشفت عنه التطبيقات العملية مثل نظام *COMPAS* القضائي، والذي أظهر تحيزات إحصائية عنصرية منهجية تخل بمبدأ المساواة أمام القانون[20].

4- الشفافية القابلة للتنفيذ والحق في التفسير: تكرس المادة 22 من اللائحة الأوروبية (*GDPR*) ضمانة دستورية هامة تكفل حق الشخص الطبيعي في عدم الخضوع لقرار آلي بالكامل ينتج آثاراً قانونية تمسه[21]. وتتويجاً لهذا التوجه، أصدرت هيئة حماية البيانات الهولندية في أبريل 2026 مبادئ توجيهية ملزمة تحدد المعايير الفنية والتفسيرية الواجب توفرها في "الحق في التفسير" ليكون القرار الحسابي خاضعاً للمساءلة القانونية[22].

5- المساءلة وتحديد المسؤولية القانونية: يفترض العقد الرقمي وجود "فاعل بشري مسؤول" في نهاية السلسلة البرمجية لتحديد المسؤولية المدنية والجنائية عند حدوث أي أضرار ناتجة عن تطبيقات الذكاء الاصطناعي. وفي هذا السياق الرقابي، وسّعت التعديلات التشريعية الدولية الصادرة في مايو 2026 من نطاق الغرامات الردعية لتصل إلى 3% من إجمالي حجم التداول العالمي السنوي للجهات المخالفة[23].

ISSN: 2352-975X ——————————EISSN: 2588-2368

ثالثاً: مؤسسات الحوكمة- من رقابة القضاء إلى هيئات مستقلة للتدقيق الخوارزمي

إن نقل العقد الاجتماعي الرقمي من الأفق النظري إلى الحيز التطبيقي يقتضي بناء هيكلية مؤسساتية مركبة؛ تماشياً مع ما أشارت إليه توصية اليونسكو بشأن ضرورة إيجاد "آليات حوكمة ومراقبة مستقلة تكفل الشفافية والرقابة الفعالة والمساءلة". ويمكن رسم هذه البنية المؤسساتية عبر ثلاث طبقات متكاملة:

1- قضاء رقمي متخصص: تُسند إليه سلطة الفصل في الطعون الموجهة ضد القرارات الخوارزمية المؤتمتة، وفحص مدى التزام الأجهزة التنفيذية بمعايير الضرورة والتناسب. وقد شددت المبادئ الدولية على حتمية وجود رقابة قضائية مستقلة، ومسبقة، وفعالة على كافة إجراءات المراقبة التقنية السيادية[24].

2- هيئات مستقلة لحماية الحقوق الرقمية: يتجاوز دورها إيقاع العقوبات المالية التقليدية ليمتد نحو ممارسة سلطة "الترخيص المسبق" للأنظمة البرمجية عالية الخطورة والإشراف الهيكلي المستمر على المنظومات الحسابية العامة.

3- التدقيق الخوارزمي الإلزامي: فرض إجراء مراجعات دورية للأنظمة من قِبل جهات تقنية محايدة لفحص جودة البيانات ومدى سلامتها من الانحياز، وقياس معدلات الخطأ الإحصائي، تماشياً مع معايير منظمة التعاون الاقتصادي والتنمية (*OECD*) التي توجب أن تكون المنظومات الرقمية وتطبيقات الذكاء الاصطناعي "قوية، وآمنة، وموثوقة" طوال دورة حياتها التشغيلية[25].

رابعاً: إعادة تعريف الخصوصية- من "سرّية البيانات" إلى "سيادة الشخص على ملفه الرقمي"

لم تعد الخصوصية في بيئة القرين الرقمي مجرد حق سلبي يقتصر على حجب المعلومات أو إبقائها سرية، بل تحولت في الفقه الحديث إلى حق إيجابي يتمثل في "السيادة الشاملة للشخص على ملفه الرقمي" وقدرته على التحكم بالصورة المستنتجة عنه خوارزمياً. وتكرس المواد من 15 إلى 22 من اللائحة العامة لحماية

البيانات (*GDPR*) حزمة من الحقوق السيادية؛ تشمل حق الوصول (المادة 15)، وحق التصحيح (المادة 16)، وحق الاعتراض على التنميط (المادة 21)، وحق طلب المراجعة البشرية (المادة 22)، فضلاً عن حق المحو الرقمي أو ما يُعرف بالحق في النسيان (المادة 17)[26]. وتأكيداً على هذا المنحى الحمائي، قضت محكمة العدل الأوروبية بأن الحق في تلقي "معلومات ذات دلالة حول المنطق الرياضي الكامن وراء" القرار الآلي يجب أن يُفسر بمعناه الواسع الذي يمكّن المواطن من فهم كنه القرار والتحقق من سلامته القانونية[27] .

خامساً: الأمن السيبراني كشرط موضوعي لصون الحرية

في الفضاء السيبراني المعاصر، يغدو الأمن السيبراني شرطاً موضوعياً لا غنى عنه لممارسة الحرية، مما يستدعي من الناحية التشريعية التمييز الحاسم بين مستويين متناقضين: أمن سيبراني دفاعي يستهدف حماية البنى التحتية وصون حرمة الحقوق الرقمية للأفراد، وأمن رقابي توسعي يتخذ من التقنية ذريعة للتغول وانتهاك الحريات. وتقتضي السياسة التشريعية الرشيدة توجيه الاستثمارات السيادية نحو تعزيز الأمن الدفاعي الشامل، مع إبقاء التدابير الرقابية كخيار استثنائي وأخير يخضع بصرامة للإذن القضائي المسبق[28].

سادساً: التربية الرقمية ومواجهة فجوات اللامساواة الخوارزمية

يكشف التحليل التلوي الشامل[29] لتقارير اليونسكو الصادرة في عام 2026 أن 83% من المنظومات القانونية الدولية باتت توصي بإجراءات تشريعية لتعزيز التنوع الرقمي ومكافحة التمييز الخوارزمي، في حين ربطت 87% من هذه التقارير بين حوكمة أخلاقيات التقنية وتأهيل سوق العمل لمواجهة تحولات الذكاء الاصطناعي[30]. ومن ثم، تصبح التربية الرقمية جزءاً لا يتجزأ من الجيل الجديد لحقوق الإنسان، بهدف رفع الوعي المجتمعي وتمكين المواطن من فهم آليات التنميط والامتلاك المعرفي لأدوات الطعن في القرارات المؤتمتة.

ISSN: 2352-975X ——————————EISSN: 2588-2368

- نحو عقد اجتماعي رقمي جديد:

إن مستقبل القرين الرقمي وتطبيقات الذكاء الاصطناعي لا ينبغي أن يغدو قدراً أمنياً محتوماً يقود نحو مجتمعات المراقبة، بل يجب تطويعه كمجال حيوي لتحديث بنيان الدولة نحو نموذج "الدولة الذكية العادلة" لا "الدولة المتلصصة". ويكمن جوهر الحل في مأسسة حوكمة التقنية عبر ثلاثة ركائز: نص قانوني جازم يحدد الغايات السيادية دون غموض، ومؤسسات رقابية مستقلة تمتلك الأدوات المعرفية لتفكيك وشرح الخوارزميات، وحقوق رقمية أصيلة قابلة للممارسة الفعلية والتقاضي الناجز، مسنودة بأمن سيبراني دفاعي صلب. فالدولة تكتسب ذكاءها المشروع حين تسخّر الأنظمة الرقمية لتطوير المرفق العام وإقرار العدالة التنبؤية المنصفة، بينما يظل المجتمع حراً طالما امتلك مواطنوه سلطة السيادة الكاملة على هويتهم وقرينهم الرقمي.

خاتمـة:

خلصت هذه الدراسة إلى أن "القرين الرقمي"، بوصفه بنية بياناتية- حسابية ديناميكية تُنتج آثاراً قانونية مباشرة على مركز الفرد، قد تجاوز كونه مجرد تمثيل تقني ليصبح موضوعاً للسيادة المتقاطعة بين الدولة والشركات والمنصات الرقمية. وقد أثبت التحليل أن إخضاع هذا الكيان لمنطق القانون والأخلاق لا يمكن أن يتم بمعزل عن إعادة تعريف لمبادئ الشرعية والضرورة والتناسب في البيئة الحسابية، ذلك أن النماذج التنبؤية المستخدمة في السياقات الأمنية، حين تُترك دون ضوابط تشغيلية وقضائية صارمة، تؤدي إلى تحول الخصوصية الفردية من حق أساسي إلى استثناء قابل للاختراق الدائم، وإلى تكريس التمييز الكمي بوصفه أداة سيادية جديدة لإدارة المخاطر وإعادة إنتاج التفاوت الاجتماعي.

انطلاقاً من هذه النتائج، تؤكد الدراسة أن التوازن بين متطلبات الأمن القومي وحقوق الإنسان في فضاء تتوزع فيه السيادة لا يمكن أن يتحقق من خلال خطاب نثري عام، بل عبر آليات قانونية مؤسسية ملزمة. لذلك تستخلص الدراسة النقاط

التالية:

أولاً: يستوجب الاعتراف بالقرين الرقمي بوصفه "مصلحة قانونية محمية" ذات طبيعة مزدوجة: فهي من جهة تدخل في نطاق الحق في الخصوصية والكرامة الإنسانية كما تفسرها المحاكم الدستورية والدولية، ومن جهة أخرى تشكل مورداً استراتيجياً للدولة في إدارة الأمن الاستباقي، مما يستدعي معالجتها تشريعياً بوصفها موضوعاً لقواعد آمرة لا يجوز التفويض الكلي فيها للجهات التقنية الخاصة.

- ثانياً: تثبت الدراسة ضرورة الانتقال من مبدأ "الموافقة الفردية التلقائية" كمبرر لمعالجة البيانات إلى مبدأ "الترخيص المؤسسي الخاضع للرقابة"، خاصة في الحالات التي تستخدم فيها الدولة النماذج التنبؤية لأغراض أمنية وسيادية. ويعني ذلك إخضاع أي نظام للمراقبة الحسابية لإذن قضائي مسبق، محدد زمناً وموضوعاً، مع إمكانية تجديده وفق معايير موضوعية لا تترك للسلطة التنفيذية هامشاً لتوسيع الاستثناءات بذريعة الضرورة الطارئة.

- ثالثاً: توصي الدراسة بإدراج ثلاث ضمانات إجرائية جوهرية في التشريعات الوطنية الحاكمة للمجال الرقمي:

1- الحق في التفسير البشري للقرارات المؤتمتة ذات الأثر القانوني الجسيم، بما يسمح للفرد بفهم المنطق الحسابي للتصنيف أو تقدير المخاطر المنسوب إليه، والطعن في سلامته الإجرائية أمام جهة قضائية مستقلة.

2- إلزامية التدقيق الحسابي المستقل للأنظمة البرمجية التي تعالج الأقران الرقمية في المجالين الأمني والقضائي، مع نشر تقارير دورية شفافة عن نسب الخطأ الإحصائي، وتحيزات البيانات، وفروق المعاملة بين الفئات السكانية.

3- إنشاء هيئات وطنية مختلطة (قضائية-تقنية) تتولى الإشراف على استخدام المنظومات الحسابية المتقدمة في وظائف السيادة، مع منحها صلاحية إيقاف أي نظام برمي يثبت تسببه في ضرر جسيم أو تمييز منهجي ضد الأفراد.

ISSN: 2352-975X ——————————EISSN: 2588-2368

رابعاً: تدعو الدراسة إلى تجاوز النهج الوطني المنفرد في حوكمة القرين الرقمي، والعمل على تنسيق إقليمي ودولي لمواجهة التحديات الناشئة عن عبور تدفقات البيانات للحدود وتوزع السيادة بين الدول والشركات العابرة للقارات. ويشمل ذلك وضع معايير دنيا لحقوق الإنسان الرقمي في اتفاقيات متعددة الأطراف، وتطوير آليات للتعاون القضائي المشترك في مجال الطعون البرمجية العابرة للحدود.

ختاماً، تفتح هذه الدراسة آفاقاً للبحث المقارن حول كيفية تحويل مبادئ الشرعية والتناسب إلى متطلبات تقنية وهندسية قابلة للتنفيذ صلب المنظومة البرمجية، وإلى تطوير نظريات قانونية تتجاوز ثنائية "الشخص الطبيعي/الشخص الاعتباري" التقليدية لتستوعب فاعلين رقميين جدداً (كالنماذج التنبؤية والأطر الحسابية السيادية) ضمن منظومة المسؤولية المدنية والجنائية. كما تؤكد على ضرورة مقاربة التوازن بين الأمن والحقوق ليس بوصفه معادلة رياضية جامدة، بل بوصفه عملية سياسية وقانونية مستمرة، تتغير بتغير المخاطر وتطور التقنيات وتوازن القوى بين الفاعلين في الساحة الدولية.

الهوامـش والمراجـع:

(1)- Rodotà, Stefano. La vita e le regole: Tra diritto e non diritto. Milano: Feltrinelli, 2006.

(2)- Solove, Daniel J. The Digital Person: Technology and Privacy in the Information Age. New York: New York University Press, 2004.

(3)- Hildebrandt, Mireille. Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology. Cheltenham-Northampton: Edward Elgar Publishing, 2015.

(4)- UN Human Rights Council. "The right to privacy in the digital age." Report of the Office of the United Nations High Commissioner for Human Rights, A/HRC/27/37, June 30, 2014.URL: https: //web.dev.ohchr.un-icc.cloud/en/documents/thematic-reports/ahrc2737-right-privacy-digital-age-focus-surveillance-report-office

(5)- Lyon, David. Surveillance Society: Monitoring Everyday Life. Buckingham-Philadelphia: Open University Press, 2001.

(6)- Zuboff, Shoshana. The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. New York: PublicAffairs, 2019.

(7)- DeNardis, Laura. The Global War for Internet Governance. New Haven-London: Yale University Press, 2014.

(8)- Richards, Neil M., and Jonathan H. King. "Big Data Ethics." Wake Forest Law Review 49, no. 2 (2014): 393-432.
(9)- Wachter, Sandra, Brent Mittelstadt, and Luciano Floridi. "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation." International Data Privacy Law 7, no. 2 (2017): 76-99.
(10)- Council of Europe. Guidelines on the Protection of Individuals with regard to the Processing of Personal Data in a World of Big Data. Strasbourg: Council of Europe Publishing, 2017.
(11)- Messier, Michaela. "AI in the Public Sector: Balancing Innovation with Constitutional Rights." Journal of Law and Public Policy Blog, University of St. Thomas, March 12, 2025. URL:
https: //blogs.stthomas.edu/jlpp-blog/page/2/#ftnref38
(12)- Jones Walker LLP. "AI Police Surveillance Bias: The 'Minority Report' Impacting Constitutional Rights." October 17, 2025. URL:
https: //www.joneswalker.com/en/insights/blogs/ai-law-blog/ai-police-surveillance-bias-the-minority-report-impacting-constitutional-right.html
(13)- . UN Human Rights Committee. "General Comment No. 16: Article 17 (Right to Privacy)." HRI/GEN/1/Rev.1, adopted April 8, 1988. URL:
https: //www.globalhealthrights.org/instrument/hrc-general-comment-no-16-article-17-right-to-privacy/
(14)- International Principles on the Application of Human Rights to Communications Surveillance (Necessary and Proportionate Principles). Launched at the 24th Session of the UN Human Rights Council, September 2013. URL:
https: //www.accessnow.org/surveillance-and-human-rights-principles-are-launched-at-the-24th-hrc/
(15)- UN Human Rights Council. "The right to privacy in the digital age." Reports A/HRC/28/39 (2014), A/HRC/39/29 (2018), A/HRC/48/31 (2021), A/HRC/51/17 (2022), A/HRC/56/45 (2024), A/HRC/60/45 (2025). URL:
https: //www.ohchr.org/en/privacy-in-the-digital-age/reports
(16)- Zuheir. "Micro-targeting in Political Campaigns: Between Democratic Communication and Manipulation." Journal of Digital Ethics 3, no. 1 (2023): 45-62.
(17)- Prasad, Khushbu, and Taru Mishra. "Reclaiming Control in Cyberspace: An Overview of Digital Sovereignty and its Global Evolution." International Journal of Law Management & Humanities 8, no. 3 (2025): 2247-2254. URL:
https: //ijlmh.com/paper/reclaiming-control-in-cyberspace-an-overview-of-digital-sovereignty-and-its-global-evolution/
(18)- TrustArc. "The Global Rise of Data Localization: Risks, Tradeoffs, and What Comes Next." September 8, 2025.
URL: https: //trustarc.com/resource/global-rise-data-localization-risks/
(19)- UN Human Rights Council. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression." A/HRC/41/35, 2019.URL:
https: //right-docs.uwazi.io/en/entity/6o2p8hhuc4m/toc?file=1612900079864oubx15k47k.pdf&page=8
(20)- European Parliament and Council of the European Union. "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the

ISSN: 2352-975X ——————————EISSN: 2588-2368

protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)." Official Journal of the European Union L 119, May 4, 2016.
URL: https: //eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX: 02016R0679-20160504
(21)- Bodewits, Joke, Julian Flamant, and July Baltus. "Dutch DPA draft guidelines on the right to explanation in ADM - Key takeaways." Hogan Lovells, April 26, 2026.URL: https: //www.hoganlovells.com/en/publications/dutch-dpa-draft-guidelines-on-the-right-to-explanation-in-adm-key-takeaways
(22)- Court of Justice of the European Union. "Opinion of Advocate General Richard de la Tour in Case C-203/22, CK v Dun & Bradstreet Austria GmbH." September 12, 2024. ECLI: EU: C: 2024: 738. URL:
https: //eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX: 62022CC0203
(23)- European Parliament and Council of the European Union. "Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act)." Official Journal of the European Union L, 2024. URL:
https: //gdprlocal.com/de/europe-ai-act-summary/
(24)- UNESCO. "Recommendation on the Ethics of Artificial Intelligence." Paris: UNESCO, November 24, 2021. SHS/BIO/PI/2021/1.
URL: https: //www.unesco.org/ethics-ai/en
(25)- Inside Privacy. "EU AI Act Update: Timeline Relief, Targeted Simplification, and New Prohibitions." May 17, 2026.
URL: https: //www.insideprivacy.com/artificial-intelligence/eu-ai-act-update-timeline-relief-targeted-simplification-and-new-prohibitions/
(26)- OECD. "Recommendation of the Council on Artificial Intelligence." OECD/LEGAL/0449. Adopted May 22, 2019 (as updated by 49 Adherents as of April 2026).
URL: https: //www.reviewofailaw.com/Tool/Evidenza/Single/viewhtml?id evidenza =5764
(27)- UNESCO. "Meta-Analysis of UNESCO Readiness Assessment Methodology (RAM) Reports." Paris: UNESCO, 2026.
URL: https: //www.unesco.org/ethics-ai/en/node/321
(28)- Borenstein, Michael, Larry V. Hedges, Julian P. T. Higgins, and Hannah R. Rothstein. Introduction to Meta-Analysis. 2nd ed. Chichester: John Wiley & Sons, 2021.

(29)- يُقصد بـ "التحليل التلوي(Meta-Analysis) " في منهجية البحث الكمي، الأسلوب الإحصائي الذي يجمع نتائج عدد من الدراسات المستقلة حول موضوع محدد، ويعيد تحليلها كمياً للوصول إلى استنتاجات أكثر دقة وثباتاً مما يمكن أن تقدمه دراسة منفردة. وقد تطوّر هذا المفهوم في الأصل من حقول الطب والعلوم التجريبية، ثم انتقل ليشمل العلوم الاجتماعية والسياسية والقانونية، حيث بات يُستخدم لاستخلاص أحجام تأثير مجمعة (Pooled Effect Sizes) من دراسات متباينة العينات والمنهجيات. وتكمن قوة هذا الأسلوب في قدرته على تجاوز محدودية النتائج المفردة التي قد تتأثر بحجم

العينة أو الخلفية السياقية للدراسة الواحدة، والوصول بدلاً من ذلك إلى تقديرات كمية إجمالية تخضع لاختبارات الدلالة الإحصائية المعترف بها دولياً. وقد أظهرت تطبيقات هذا المنهج في سياق حوكمة الذكاء الاصطناعي، قدرتها على تحويل مجموعة من التقارير الوطنية أو الإقليمية (مثل تقارير تقييم الجاهزية الصادرة عن اليونسكو) إلى مؤشرات رقمية قابلة للمقارنة والتحليل، مما يعزز من الطابع العلمي للاستنتاجات ويخرج بها من دائرة الرأي أو التوصيف النوعي المجرد إلى دائرة البرهان الإحصائي القابل للتحقق والمراجعة.

(30)- Electronic Frontier Foundation. Electronic Frontier Foundation Annual Report 2022. San Francisco: Electronic Frontier Foundation, 2022. United Nations. International Covenant on Civil and Political Rights. General Assembly resolution 2200A (XXI), December 16, 1966, in force since March 23, 1976. URL: https: //www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights; European Union Agency for Fundamental Rights (FRA). Fundamental Rights Report 2025. URL: https: //fra.europa.eu/en/publication/2025/fundamental-rights-report-2025