مجلة

جامعة شندي

للبحوث والدراسات الشرعية والقانونية

(علمية – نصف سنوية – محكمة)

تصدر عن كلية القانون جامعة شندي

العدد الثاني عشر - يوليو ٢٠٢٥م


بسم الله الرحمن الرحيم

الإشراف العام :

عمادة البحث العلمي بالجامعة

الهيئة الإستشاريَّة :

أ.د. إبراهيم حسن إبراهيم

أ.د. أحمد المصطفى محمد صالح

أ.د. أسامة محمد عثمان خليل

أ.د. أسعد عبد الحميد إبراهيم

أ.د. الحاج محمد الحاج الدوش

أ.د. جلال الدين بانقا أحمد بشير

أ.د. سيف الدين الياس حمدتو أرباب

أ.د. شهاب سليمان عبد الله

أ.د. عوض أحمد إدريس

رئيس هيئة التحرير :

أ.د. عمر الجيلاني الأمين حماد.

مدير التحرير :

د. عمر مختار سالم عبد الرحمن

عضوية هيئة التحرير :

د. هويدا خلف الله حسين

أ. نسيبة إبراهيم محمد عبد القادر

مساعدو التحرير :

أ. أميمة فاروق عثمان الحسين

أ. تسابيح بابكر عبد الله

المراجعة اللغويَّة :

د. صديق خالد الحاج

قواعد وإجراءات النشر في المجلة

أولاً/ القواعد العامة لقبول النشر:

١. أن يكون البحث أصيلاً ، وتتوافر فيه شروط البحث العلمي المعتمد على الأصول العلمية والمنهجية المتفق عليها في كتابة البحوث الأكاديمية شكلاً ومضموناً .
٢. أن يكون البحث بلغة سليمة، ومراعياً لقواعد الضبط ، والموضوعية والمستوى العلمي الرفيع ، وألا تزيد صفحاته عن (٣٥) صفحة متضمنةً الهوامش والمراجع .
٣. أن يكون الباحث ملتزماً بدقة التوثيق ، وحسن إستخدام المصادر والمراجع ، وتثبيت الهوامش والمراجع في نهاية كل صفحة .
٤. ألا يكون البحث قد سبق نشره أو قُدِّم للنشر في أي جهة أخرى.
٥. للمجلة الحق في إخراج البحث وإبراز عناوينه بما يتناسب وأسلوبها في النشر.
٦. يرفق ملخص البحث المراد نشره فى حدود (١٠٠- ١٥٠) كلمة باللغتين العربية والإنجليزية ، ويكون مسبوقاً بالعنوان ، ويوضع فى صفحة منفصلة .

ثانياً/ إجراءات النشر:

١. يرسل البحث مطبوعاً ومراجعاً من نسختين مع المادة المحفوظة في أقراص الحاسوب المرنة أو المدمجة أو على ايميل المجلة.
٢. في حالة قبول البحث مبدئياً يتم عرضه على محكّمين اثنين من ذوي الاختصاص في مجال البحث ، ويتم إختيارهم بسرية تامة ، ولا يعرض عليهم إسم الباحث أو بياناته ، وذلك لإبداء آرائهم حول مدى أصالة البحث وقيمته العلمية.
٣. يخطر الباحث بقرار صلاحية بحثه للنشر من عدمها على ضوء قرار المحكَّمين .
٤. في حالة ورود ملاحظات من المحكَّمين ترسل تلك الملاحظات إلى الباحث لإجراء التعديلات اللازمة ، على أن تعاد للمجلة خلال مدة أقصاها شهر من إستلامه تلك الملاحظات .
٥. البحوث التي لم تنشر لا تعاد للباحثين .
٦. ظهور البحث وترتيبه في المجلَّة يخضع للإعتبارات الفنيَّة.

ثالثاً/ حقوق النشر:

تؤول حقوق النشر كافة للمجلة .

رابعاً/ المسئولية القانونية عن النشر:

تعبِّر جميع الأفكار الواردة في البحوث المنشورة في المجلة عن آراء كاتبيها ولا تعبِّر عن وجهة نظر المجلة.

مراسلة المجلة على العنوان التالي:

جامعة شندى – كليَّة القانون - مجلة جامعة شندي للدراسات والبحوث الشرعيَّة والقانونيَّة

ص.ب ١٤٢ ، ١٤٣ . شندى . السودان

البريد الألكترونى: journal.law2017@gmail.com

كلمة العدد

في ظروف بالغة التعقيد سعينا لأن نواصل جهدنا خدمة للعلم والعلماء إيماناً منا بأهمية النشر و بضرورة السعي لتخطي الصعاب .

بين ثنايا هذا العدد مجموعة من البحوث تنوعت موضوعاتها في المجالات الشرعية والقانونية كما تعددت مدارس كتابها و نواحي وجودهم المكاني كانت خيار ما وصل الينا بعد أن تم إعمال قلم التحكيم الصارم الذي استبعد من النشر ضعف ما هو منشور .

ما زالت أبواب مجلتنا مفتوحة لاستقبال البحوث والدراسات في المجالات الشرعية والقانونية و ما تزال دعوتنا قائمة للكتاب والباحثين من مختلف أنحاء الوطن العربي والإسلامي بل والعالم كله للكتابة و النشر عبر هذه النافذة التي نرجو أن تكون من النوافذ العلمية المهمة والمفيدة.

بإذن الله ستشهد الفترة القادمة جملة من الترتيبات الإدارية والفنية في سبيل الحفاظ على ما أنجز سابقاً و سعياً للتطوير و التجويد.

جزيل الشكر لكل من أسهم في إعداد و إخراج هذا العدد و الأعداد السابقة و لكل الذين أسهموا بالتحكيم ، و الشكر موصول لكل من منحنا ثقته وتوجه الينا قاصداً النشر عبر مجلتنا والله نسأله التوفيق والسداد.

رئيس التحرير

فهرست البحوث في العدد الثاني عشر

م	الموضوع	الكاتب	الصفحة
١.	الحماية القانونية للمدنيين وفق قانون النزاع المسلح (دراسة تحليلية لقواعد القانون الإنساني الدولي مقارنة مع التشريع السوداني)	١/ أ.د. شهاب سليمان عبد الله. ٢/ د. فيروز عوض الكريم صالح	٨
٢.	أثر تجاوز الاختصاص فى عمل مجلس الأمن على القضاء الجنائى الدولى	أ.د. زكريا عبد الوهاب محمد زين	٤٠
٣.	الاطار القانوني لحماية الخصوصية و البيانات الشخصية في عصر الذكاء الاصطناعي دراسة تحليلية على ضوء قانون جرائم المعلوماتية السوداني والتشريعات المقارنة	١/ د. أبوعبيده الطيب سليمان الخليفة ٢/ د. أسعد محمد قاسم احمد ٣/ د. معتز الصادق سلمان	٧٤
٤.	أحكام الدفاع الشرعي في قانون الجزاء العماني رقم (٢٠١٨/٧م)	١/ د. صابرين جابر محمد ٢/ د. حازم أبو الحمد حمدي	١٠٧
٥.	قصص إحياء الموتى في سورة البقرة	د. معاوية عبد الكريم محمد سلمان	١٢٥
٦.	مدى جدية الحماية القانونية لمواجهة الاضرار بالبيئة قبل انعكاسها السلبي على الأنسان والتنمية	د. سالم احمد مسلم حار الكثيري	١٤٢

الاطار القانوني لحماية الخصوصية و البيانات الشخصية في عصر الذكاء الاصطناعي
دراسة تحليلية على ضوء قانون جرائم المعلوماتية السوداني والتشريعات المقارنة

١/ د. أبوعبيده الطيب سليمان الخليفة

أستاذ مشارك – عميد كلية القانون – جامعة النيلين - السودان

٢/ د. أسعد محمد محمد قاسم محمد

استاذ مساعد - كلية القانون – جامعة النيلين – السودان

٣/ د. معتز الصادق محمد سلمان

مستشار وخبير قانوني – الدوحة – دولة قطر

مستخلص البحث

يهدف هذا البحث إلى استجلاء الإطار القانوني لحماية الخصوصية والبيانات الشخصية في السودان في ظل التسارع المتنامي لتقنيات الذكاء الاصطناعي، وذلك من خلال تحليل نصوص قانون مكافحة جرائم المعلوماتية وتعديلاته، ومقارنتها بالاتجاهات التشريعية المعاصرة، ولا سيما اللائحة الأوروبية لحماية البيانات (GDPR) والتشريعات الخليجية الحديثة في كلٍّ من دولة الإمارات العربية المتحدة والمملكة العربية السعودية ودولة قطر. وتنطلق الدراسة من إشكالية محورية تتمثل في مدى كفاية المنظومة القانونية السودانية الراهنة لتوفير حماية فعّالة للبيانات الشخصية في عصر المعالجة الخوارزمية، في ظل غياب تشريع شامل لحماية البيانات واتساع نطاق المخاطر الناشئة عن استخدام الأنظمة الذكية في جمع البيانات وتحليلها واستنتاجها. وقد اعتمد البحث منهجاً تكاملياً يجمع بين المنهج الوصفي لرصد الإطار القانوني القائم، والمنهج التحليلي لتفكيك المفاهيم التقنية والقانونية المرتبطة بالذكاء الاصطناعي ومعالجة البيانات، والمنهج المقارن لاستعراض النماذج الدولية والخليجية، والمنهج الاستقرائي لاستخلاص الحلول التشريعية الملائمة للواقع السوداني. وتخلص الدراسة إلى أن الحماية القانونية للبيانات الشخصية في السودان ما تزال مجتزأة وغير منسجمة، إذ تقوم على نصوص دستورية ومدنية عامة وأحكام عقابية متفرقة في قانون جرائم المعلوماتية، وهي نصوص لا تواكب طبيعة المخاطر المعاصرة المرتبطة بالتعلم الآلي، والتنبؤ السلوكي، والتصنيف الخوارزمي، والقرارات المؤتمتة. كما يبرز البحث تميز التجارب المقارنة في إرساء منظومات متكاملة تقوم على تعريفات دقيقة للبيانات، وتكريس حقوق موسعة للأفراد، وإنشاء هيئات رقابية مستقلة، ووضع ضوابط صارمة للمعالجة والقرارات الآلية. وبناءً

عليه، يوصي البحث بضرورة التعجيل بإصدار قانون سوداني خاص بحماية البيانات الشخصية، مؤسس على مبادئ الموافقة المستنيرة، والشفافية، والمساءلة، وأمن البيانات، وتقييد المعالجة والقرارات المؤتمتة، مع إنشاء هيئة وطنية مستقلة للإشراف والرقابة، ومواءمة التشريع الوطني مع المعايير الدولية والتجارب الخليجية، وتنظيم تطبيقات الذكاء الاصطناعي عالية المخاطر في القطاعات الحيوية، بما يحقق التوازن بين الابتكار التكنولوجي وصون الحقوق والحريات الأساسية.

Abstract

This study examines the legal framework for the protection of privacy and personal data in Sudan in light of the rapid expansion of artificial intelligence (AI) technologies. It analyzes the provisions of the Cybercrime Act and its amendments, and compares them with contemporary legislative trends, particularly the European General Data Protection Regulation (GDPR) and recent data protection laws adopted in the Gulf region, notably in the United Arab Emirates, the Kingdom of Saudi Arabia, and the State of Qatar.The research is grounded in a central question concerning the adequacy of the current Sudanese legal framework in ensuring effective protection of personal data in the era of algorithmic processing. This question is especially pressing given the absence of a comprehensive data protection statute and the increasing risks posed by intelligent systems used for data collection, analysis, inference, and automated decision-making.An integrated methodological approach is employed, combining the descriptive method to identify the existing legal framework, the analytical method to examine the technical and legal concepts associated with artificial intelligence and data processing, the comparative method to assess international and Gulf legislative models, and the inductive method to derive legislative solutions appropriate to the Sudanese legal context.The study finds that personal data protection in Sudan remains fragmented and insufficiently coherent. It relies primarily on general constitutional and civil law provisions, alongside dispersed criminal norms contained in the Cybercrime Act. These provisions do not adequately address contemporary risks associated with machine learning, behavioral prediction, algorithmic profiling, and automated decision-making systems. By contrast, the comparative legislative models demonstrate more comprehensive and structured frameworks, characterized by precise definitions of personal data, the recognition of expanded data subject rights, the establishment of independent supervisory authorities, and the imposition of strict safeguards governing data processing and automated decisions.Accordingly, the study recommends the prompt enactment of a dedicated Sudanese Personal Data Protection Law grounded in the principles of informed consent, transparency, accountability, data security, and the regulation of automated processing and decision-making. It further calls for the establishment of an independent national supervisory authority, the harmonization of domestic legislation with international standards and relevant Gulf experiences, and the regulation of high-risk AI applications in critical sectors, in a manner that balances technological innovation with the protection of fundamental rights and freedoms.

مقدمة:

يشهد العالم في العقود الأخيرة تحولاً جذرياً تقوده تقنيات الذكاء الاصطناعي والأنظمة القائمة على تحليل البيانات، وهي تقنيات لم تعد مجرد أدوات مساعدة، بل أصبحت بنية أساسية تخترق مختلف القطاعات الحكومية والخاصة، وتعيد تشكيل طرق جمع البيانات وتحليلها وتوظيفها في اتخاذ القرارات. وقد مكنت هذه الأنظمة من تتبع السلوك البشري، واستنتاج الأنماط والميول، بل والولوج إلى طبقات عميقة من المعلومات الشخصية الحساسة التي قد يجهلها صاحبها نفسه، الأمر الذي جعل الحق في الخصوصية وحماية البيانات الشخصية من أكثر الحقوق عرضة للانتهاك في العصر الرقمي.

وفي السودان يزداد هذا التحدي تعقيداً في ظل غياب إطار قانوني شامل ومتخصص ينظم حماية البيانات الشخصية بصورة متكاملة، واعتماد المنظومة القانونية الحالية على نصوص محدودة ومتفرقة، أبرزها ما ورد في قانون مكافحة جرائم المعلوماتية لسنة ٢٠١٨ تعديل ٢٠٢٥م، إلى جانب بعض النصوص الدستورية ذات الطابع العام التي لا تستجيب للمتطلبات التفصيلية اللازمة لضمان حماية فعالة للخصوصية في ظل عصر الذكاء الاصطناعي.

ويفاقم هذا القصور التشريعي توسع الجهات الحكومية والخاصة في تبني الأنظمة الذكية ومسارات التحول الرقمي دون وجود قانون خاص يحدد ضوابط جمع البيانات ومعالجتها وتخزينها وإتاحتها، وهو ما يُعمق المخاطر المرتبطة بإساءة استخدام البيانات الشخصية أو استغلالها خارج الأغراض المشروعة، ويُضعف الثقة العامة في البيئة الرقمية، ويجعل الأفراد أكثر عرضة لانتهاكات قد تمس حقوقهم الأساسية في الخصوصية وصون الحياة الخاصة.

وتثير هذه المعطيات مجتمعة تساؤلاً محورياً وجوهرياً حول مدى قدرة المنظومة القانونية السودانية الراهنة على مواكبة التطور المتسارع لتقنيات الذكاء الاصطناعي، ومدى جاهزيتها لتوفير حماية فعالة وشاملة للبيانات الشخصية في ظل التحولات التقنية المتعاظمة واتساع نطاق مخاطرها.

وانطلاقاً من هذه الإشكاليات، تأتي هذه الدراسة لتحليل الإطار القانوني لحماية الخصوصية والبيانات في السودان، والكشف عن مواطن القصور التي تحد من فعاليته،

والوقوف على أبرز التجارب التشريعية المقارنة - الإقليمية والدولية - التي يمكن الاسترشاد بها.

أهمية الدراسة :

تنبع أهمية هذه الورقة من كونها تتناول أحد أكثر الموضوعات إلحاحاً في البيئة القانونية المعاصرة، وهو حماية الخصوصية والبيانات الشخصية في ظل التطور المتسارع لتقنيات الذكاء الاصطناعي، ويكتسب هذا الموضوع أهمية خاصة في السودان، حيث يشهد البلد توسعاً متزايداً في تبنّي التطبيقات الرقمية والأنظمة الذكية دون وجود إطار تشريعي متكامل ينظم جمع البيانات ومعالجتها ويضمن حماية الحقوق الرقمية للأفراد.

مشكلة الدراسة :

على الرغم من أن الذكاء الاصطناعي أصبح أحد أهم الأدوات التقنية في إدارة البيانات وتحليلها واتخاذ القرار، إلا أن استخدامه الواسع أثار تحديات قانونية وأخلاقية عميقة تتعلق بحماية الخصوصية والبيانات الشخصية.

وفي السياق السوداني، تتفاقم هذه التحديات نتيجة غياب إطار تشريعي متكامل لحماية البيانات، واقتصار الحماية على أحكام متناثرة في قانون مكافحة جرائم المعلوماتية وبعض النصوص الدستورية العامة التي لا ترقى إلى مستوى التنظيم الشامل المطلوب لضبط المعالجة الرقمية الحديثة التي تفرضها تقنيات الذكاء الاصطناعي.

وبناءً على ذلك، تتمثل المشكلة الرئيسية لهذه الدراسة في السؤال الآتي:

إلى أي مدى يستطيع الإطار القانوني السوداني الحالي توفير حماية فعّالة للخصوصية والبيانات الشخصية في ظل التوسع المتزايد في استخدام تقنيات الذكاء الاصطناعي؟

أسئلة الدراسة :

١. ما المقصود بالذكاء الاصطناعي والبيانات الشخصية، وما أبرز المخاطر التي يمكن أن تنشأ عن استخدام هذه التقنيات؟
٢. ما هو الإطار القانوني السوداني المنظّم للخصوصية والبيانات الشخصية حالياً ؟، وما مدى قدرته على توفير حماية فعالة في البيئة الرقمية؟
٣. كيف تناولت التشريعات المقارنة – ولاسيما اللائحة الأوروبية لحماية البيانات (GDPR)والتشريعات الخليجية الحديثة – تنظيم حماية البيانات في ظل تطور تقنيات الذكاء الاصطناعي؟

٤. ما أوجه القصور التي تعاني منها المنظومة القانونية السودانية مقارنةً بالنماذج التشريعية الإقليمية والدولية المتقدمة؟
٥. ما المبادئ القانونية والضوابط التنظيمية التي ينبغي أن يستند إليها وضع تشريع سوداني حديث يواكب التحولات الرقمية ويضمن حماية فعّالة للبيانات الشخصية؟

أهداف الدراسة :

١. بيان الأساس القانوني لحماية الخصوصية والبيانات الشخصية في القانون السوداني.
٢. تحليل مدى كفاية وفعالية المنظومة القانونية السودانية الحالية في التصدي للمخاطر التي تفرضها تقنيات الذكاء الاصطناعي.
٣. دراسة النماذج التشريعية المقارنة، ولا سيما اللائحة العامة لحماية البيانات الأوروبية (GDPR) والقوانين الخليجية الحديثة، بهدف استخلاص المبادئ والمعايير الجديرة بالتطبيق في السياق السوداني.

منهجية الدراسة :

إعتمدت الدراسة منهجية علمية مختصرة قوامها المنهج الوصفي- التحليلي والمنهج المقارن؛ إذ استُخدم المنهج الوصفي- التحليلي لعرض المفاهيم الأساسية المرتبطة بالذكاء الاصطناعي والبيانات الشخصية، وتحليل النصوص القانونية السودانية القائمة وتقويم مدى كفايتها في مواجهة تحديات البيئة الرقمية الحديثة، بينما تم توظيف المنهج المقارن لدراسة النماذج التشريعية المتقدمة، ولا سيما اللائحة الأوروبية لحماية البيانات (GDPR) والتشريعات الخليجية الحديثة، بهدف استخلاص المبادئ والضوابط التي يمكن الاستفادة منها في تطوير الإطار التشريعي السوداني بما يتلاءم مع خصوصيته القانونية والمؤسسية.

هيكل الدراسة :

قسمت هذه الدراسة إلى ثلاثة مباحث رئيسة تكاملت فيما بينها لبناء معالجة علمية منهجية لموضوع البحث؛ خُصِّص المبحث الأول لبيان الإطار المفاهيمي والنظري لحماية البيانات الشخصية في عصر الذكاء الاصطناعي، من خلال مطلبين تناول أولهما مفهوم الذكاء الاصطناعي ودور البيانات في تشغيل أنظمته، فيما عالج ثانيهما ماهية البيانات الشخصية ومخاطر استخدامها في التطبيقات الذكية. وتناول المبحث الثاني الإطار القانوني لحماية الخصوصية والبيانات الشخصية في السودان، وذلك عبر مطلب أول خُصِّص للأساس الدستوري والمدني والجنائي للحماية، ومطلب ثانٍ عالج تنظيم

البيانات الشخصية في قانون مكافحة جرائم المعلوماتية مع تقييم مدى فعاليته في مواجهة تحديات الذكاء الاصطناعي. أما المبحث الثالث، فقد اتجه إلى استشراف إطار قانوني حديث لحماية البيانات في السودان، من خلال مطلب أول تناول الاتجاهات التشريعية المقارنة والاستفادة منها في السياق السوداني، ومطلب ثانٍ خُصِّص لبيان المبادئ القانونية الأساسية التي ينبغي تضمينها في التشريع السوداني المقترح، بما يحقق حماية فعالة للبيانات الشخصية في ظل التحول الرقمي المتسارع.

المبحث الأول

الإطار المفاهيمي والنظري لحماية البيانات الشخصية في عصر الذكاء الإصطناعي

تمثل الإحاطة بالأسس المفاهيمية للذكاء الاصطناعي وطبيعة البيانات الشخصية خطوة جوهرية لفهم التحديات القانونية التي تفرضها البيئة الرقمية المعاصرة. فقد أدى التطور المتسارع في قدرات الأنظمة الذكية إلى تحويل البيانات إلى مورد استراتيجي بالغ الأهمية، تعتمد عليه خوارزميات التحليل والتنبؤ وصنع القرار، الأمر الذي عمّق الحاجة إلى إعادة النظر في آليات حماية الخصوصية والضوابط الحاكمة لمعالجة البيانات.

وفي هذا السياق، يتناول هذا المبحث الأسس النظرية التي يقوم عليها تنظيم حماية البيانات، من خلال استعراض مفهوم الذكاء الاصطناعي وأبعاده التقنية والقانونية، وبيان ماهية البيانات الشخصية وأنواعها، وتحليل المخاطر التي تثيرها عمليات جمعها ومعالجتها في بيئة تقوم على الأتمتة والخوارزميات. ويأتي هذا من خلال المطالب التالية:

المطلب الأول/ مفهوم الذكاء الاصطناعي ودور البيانات في تشغيله :

الفرع الأول/ تعريف الذكاء الاصطناعي ونشأته وتطوره:

يُعدّ الذكاء الاصطناعي أحد أبرز مخرجات الثورة الرقمية المعاصرة وأكثرها تأثيراً في تشكيل البنية المعرفية والقانونية والاجتماعية للعصر الحديث. وقد أدى الاهتمام المتزايد به من جانب المبرمجين والفلاسفة والقانونيين إلى تعدد تعريفاته وتباينها بحسب زاوية النظر وطبيعة الاستخدام.

فعلى المستوى التقني، يُعرف الذكاء الاصطناعي بأنه:

"قدرة الأنظمة الحاسوبية على أداء المهام التي تتطلب عادةً ذكاءً بشرياً، مثل التعلم، الاستنتاج، اتخاذ القرار، والتفاعل مع البيئة".[(١)]

أما من منظور علم الحاسوب، فقد عرّفه العالم جون مكارثي - أحد المؤسسين لهذا المجال – بأنه: "علم وهندسة صناعة آلات قادرة على أداء مهام تتطلب ذكاءً بشرياً".[(٢)]

ومن منظور فقهي عربي، عرف بعض الباحثون العرب الذكاء الاصطناعي بأنه:

---

(١) د. أشرف توفيق شمس الدين، الذكاء الاصطناعي والمسؤولية القانونية، دار النهضة العربية، ٢٠٢١. ص ٨

(٢) د. عبد الفتاح بيومي حجازي، الحماية القانونية للبيانات في البيئة الرقمية، القاهرة، ٢٠٢٠. ص ١٤

"قدرة النظم الحاسوبية على محاكاة السلوك الإنساني الواعي، وإنتاج تصرفات ذكية يمكن أن تسهم في اتخاذ القرار، أو تؤثر في الحق والالتزام، بما يجعلها محل اعتبار قانوني"[١]

بينما ذهب رأي آخر إلى اعتباره:

"منظومة رقمية تتفاعل مع البيانات والتوجيهات وتقوم بمعالجتها وتنظيمها للوصول إلى نتائج معرفية قابلة للتطبيق، ومؤثرة في مراكز قانونية قائمة أو محتملة"[٢]

من خلال ما تقدم يتضح أن هذين التعريفين يمنحان مفهوم الذكاء الاصطناعي بعداً قانونياً وأخلاقياً يتجاوز كونه أداة تقنية فحسب، ليصبح منظومة قادرة على إنتاج آثار قانونية مؤثرة في المراكز والحقوق الفردية. وهو ما يفرض مقاربة أكثر عمقاً عند تناول قواعد المسؤولية والضوابط المنظمة لمعالجة البيانات، بما ينسجم مع طبيعة المخاطر التي يمكن أن تنشأ عن الأنظمة الذكية.

اما من الزاوية القانونية، لم يُجمع الفقه على تعريف موحّد، إلا أن مشروع تنظيم الذكاء الاصطناعي في الاتحاد الأوروبي لسنة ٢٠٢١ قد عرفه بأنه:

"نظام يُدار برمجياً أو يظهر في شكل مكونات مادية، قادر على استنتاج الأنماط أو اتخاذ قرارات مستقلة اعتماداً على البيانات المقدمة إليه، وذلك في سياق تحقيق أهداف محددة".[٣]

ويُلاحظ من خلال هذا التعريف أنّه يربط الذكاء الاصطناعي بعنصرين جوهريين في التحليل القانوني، هما استقلالية اتخاذ القرار وتأثيره المباشر في المراكز والحقوق الفردية، وهو ما يفتح الباب أمام تساؤلات عميقة بشأن حدود المسؤولية القانونية والضوابط التشريعية الواجب وضعها لضمان الاستخدام المنضبط والآمن لهذه الأنظمة

من ناحية أخرى، لا يكتمل فهم الذكاء الاصطناعي دون الوقوف على تطوره التاريخي؛ إذ ظهرت اللبنات الأولى له في خمسينيات القرن الماضي، لكنه ظل محدود

---

(١)سامي بشارة، "حماية الخصوصية في البيئة الرقمية"، المجلة العربية للقانون، العدد ٤، ٢٠٢١، ص ٧٧

(٢)د. محمود طارق هارون ، مدخل الى علم الذكاء الاصطناعي ، دار النشر العربية ، القاهرة ، ٢٠١٩. ص ٢٠

(٣)إيمان عبد الله، "الحق في الخصوصية في ظل الذكاء الاصطناعي"، مجلة الحقوق، جامعة القاهرة، ٢٠٢٢. ص ١٢

القدرات لعدة عقود. ومع مطلع الألفية الثالثة، ومع ظهور تقنيات التعلم الآلي (Machine Learning)والتعلم العميق(Deep Learning) ، شهد الذكاء الاصطناعي طفرة نوعية مكّنته من تحليل السلوك البشري، وبناء ملفات رقمية دقيقة للأفراد، واستنتاج أنماط اجتماعية ونفسية بالغة الحساسية.

وفي السودان، بدأت بعض المؤسسات الحكومية والقطاع الخاص في توظيف تطبيقات الذكاء الاصطناعي في مجالات متعددة، مثل أنظمة التعرّف على الهوية، والحكومة الإلكترونية، والتصنيف الأكاديمي، وتقييم المخاطر الائتمانية، وبرمجيات المراقبة الأمنية. غير ان هذا الاستخدام جاء في ظل غياب إطار قانوني متخصص ينظم جمع البيانات ومعالجتها وتداولها، الأمر الذي يجعل الأفراد عرضة لانتهاكات محتملة لحقوق الخصوصية، دون وجود ضمانات تشريعية كافية أو آليات فعالة للمساءلة القانونية.

وفي ضوء ذلك يتبيّن أن أحد أبرز التحديات في السياق السوداني يتمثل في أن التوسع في استخدام الأنظمة الرقمية والذكية قد جاء سابقاً على بناء منظومة قانونية متخصصة لحماية البيانات، الأمر الذي أسهم في اتساع الفجوة بين التطور التقني والإطار التنظيمي الناظم له. وتبرز من ثمّ الحاجة الملحّة إلى وضع تشريع حديث ومتكامل يستوعب متطلبات التحول الرقمي ويضمن حماية فعّالة لبيانات الأفراد، دون أن يشكّل ذلك عائقاً أمام مسار الابتكار التقني وتطبيقاته المتنامية

الفرع الثاني / البيانات كعنصر جوهري في تشغيل الأنظمة (الأهمية والخصائص القانونية):

أصبحت البيانات في عصر الذكاء الاصطناعي تمثل المورد الأكثر قيمة في الاقتصاد الرقمي، حتى وُصفت بأنها "نفط القرن الحادي والعشرين"، لما تؤديه من دور محوري في تشغيل الأنظمة الذكية وبناء نماذج التعلّم والتحليل والتنبؤ. فكلما ازدادت كمية البيانات ودقتها وتنوّعها، ازدادت قدرة الأنظمة على إنتاج مخرجات أكثر فعالية وتأثيراً. ومن ثمّ، فإن فهم الطبيعة القانونية لهذه البيانات يعد ضرورة أساسية قبل الانتقال إلى وضع الأطر التشريعية المنظمة لها.

وتستمد البيانات أهميتها في بيئة الذكاء الاصطناعي من مجموعة من الخصائص المميزة، أبرزها:

١- القابلية للتحليل والاستنتاج:

لا تقتصر البيانات التي تعتمد عليها الأنظمة الذكية على ما يقدمه الفرد طوعاً من معلومات صريحة، بل تمتد لتشمل البيانات المستنتجة التي تولدها الخوارزميات، مثل

الميول السياسية أو الحالة الصحية أو التوجهات السلوكية. وهذه البيانات المستنبطة غالباً ما تكون أكثر حساسية من البيانات التقليدية، لأنها تُنتج دون علم الشخص المعني.[١]

وبهذا المعنى، تُعد القدرة الاستنتاجية للأنظمة الذكية من أخطر الإشكالات القانونية المعاصرة، إذ إنها تقوض المفهوم التقليدي للموافقة المستنيرة، وتُتيح معالجة بيانات لم يفصح عنها الفرد ابتداءً، مما يوسّع نطاق المعالجة إلى حدود تتجاوز إرادته وسيطرته الفعلية على بياناته الشخصية.

٢- القابلية للتراكم والدمج عبر مصادر متعددة:

تتميّز البيانات في الأنظمة الذكية بقابليتها للدمج من عدة مصادر: منصات التواصل، السجلات الصحية، أنظمة الدفع، والموقع الجغرافي... إلخ. ويسمح هذا الدمج بتكوين صورة دقيقة وشبه كاملة عن الفرد، تُعرف بـ "البصمة الرقمية."[٢]

ويُظهر هذا التراكم المتدرّج والمتعدد المصادر للبيانات تحدياً قانونياً جوهرياً، إذ يُصعّب من ضبط حدود المعالجة وتحديد المسؤولية عن كل مرحلة من مراحلها، الأمر الذي يزيد من احتمالات المساس بالخصوصية ويُبرز الحاجة إلى وضع قواعد تشريعية دقيقة تنظم عمليّات الدمج والتجميع وتحُد من آثارها على حقوق الأفراد.

٣- الاستمرارية وصعوبة الإزالة:

تتسم البيانات الرقمية بقدرتها على البقاء، إذ يمكن حفظها واستعادتها ونقلها بسهولة، وقد تبقى مخزّنة في النسخ الاحتياطية أو قواعد البيانات الثانوية حتى بعد حذفها من المصدر الأصلي. ولذلك أصبح تطبيق "الحق في النسيان" واحداً من أكثر التحديات العملية في نظم حماية البيانات.ويرى الباحثون أن هذا الطابع الدائم للبيانات يفرض على المشرع السوداني تبني قواعد واضحة للمدة المسموح بالاحتفاظ بالبيانات خلالها، وطبيعة الإزالة الواجبة، فضلاً عن وضع التزامات تقنية على الجهات المعالجة لضمان تنفيذ الحذف الفعلي وليس الصوري.[٣]

---

(١) د. منال البلقاسي، الذكاء الصناعي – صناعة المستقبل (الحاسبات المتوازية – التحكم الالي – البرمجة الوراثية – لغة البرولوج – الخلايا العصبية)، مكتبة نور الالكترونية ، ٢٠٢٤. ص ٢٦

(٢) د. قصي حبيب ، مقدمة في الشبكات العصبية الاصطناعية ، جامعة صلاح الدين ، كردستان العراق ، ٢٠٢١. ص ١٤

(٣) أ . حسام حسن ، تاريخ الذكاء الاصطناعي ، دار النهضة العربية ، ٢٠١٢م. ص ٢١

ومن خلال تحليل هذه الخصائص، يتضح أن البيانات في بيئة الذكاء الاصطناعي لم تعد مجرد «معلومات رقمية» يجري التعامل معها كمدخلات تقنية، بل أصبحت ذات طبيعة قانونية معقّدة تستوجب إطاراً تنظيمياً متكاملًا يغطي جميع مراحل تداولها، بدءاً من جمعها مروراً بمعالجتها ودمجها، وانتهاءً بالاحتفاظ بها أو إتلافها. وتتعاظم هذه الحاجة بصورة خاصة بالنسبة للبيانات الحساسة والمستنتجة، لما تثيره من مخاطر جسيمة على الحقوق والحريات الفردية.

وبناءً على ذلك، يبرز بوضوح ضرورة وضع تشريع سوداني حديث يحدد بدقة ضوابط جمع البيانات، وأغراض استخدامها، وآليات معالجتها، وشروط الاحتفاظ بها، بما ينسجم مع مبادئ الشفافية، والموافقة المستنيرة، والحق في النسيان، بوصفها ركائز أساسية لحماية الخصوصية في العصر الرقمي.

المطلب الثاني / البيانات الشخصية ومخاطر استخدامها في تطبيقات الذكاء الاصطناعي:

الفرع الأول/ تعريف البيانات الشخصية وأنواعها:

تُعد البيانات الشخصية محور الحماية القانونية في البيئة الرقمية، وهي العنصر الأكثر تأثراً بتطبيقات الذكاء الاصطناعي. وقد قدّمت اللائحة الأوروبية لحماية البيانات (GDPR) تعريفاً شاملاً للبيانات الشخصية باعتبارها:

"كل معلومة تتعلق بشخص طبيعي محدد أو قابل للتحديد، بصورة مباشرة أو غير مباشرة، من خلال رقم تعريف، أو موقع، أو هوية جينية أو بيومترية، أو أي عامل يتعلق بهويته الجسدية أو النفسية أو الاجتماعية". [1]

ويمتاز هذا التعريف باتساعه وشموله للبيانات الظاهرة والمستترة، وهو ما يجعله ملائماً للتحديات التي تفرضها التقنيات الذكية الحديثة.

ويمكن تقسيم البيانات الشخصية في ضوء المعايير الدولية إلى أربع فئات رئيسية:

أولاً: البيانات التعريفي(Identifiable Personal Data):

وهي البيانات التي تسمح بشكل مباشر بتحديد هوية الفرد، وتشمل الاسم الكامل والرقم الوطنيالعنوان ورقم الهاتفالصورة الشخصية أو أي مُعرِّف بصريالأرقام البنكية أو الحسابية

---

(١) د. ايمن الاسيوطي ، الجوانب القانونية لتطبيق الذكاء الاصطناعي، دار النهضة العربية، ٢٠٢٤. ص ٧

وتُعد هذه الفئة الأساس في نظم الهوية التقليدية، لكنها تكتسب أهمية أكبر عندما تُدمج مع بيانات أخرى في بيئة الذكاء الاصطناعي، فتُسهم في رسم صورة دقيقة عن الشخص وسلوكه.[١]

ثانياً: البيانات السلوكية والتحليلية(Behavioral and Analytical Data)

وهي البيانات التي تُستخلص من نشاط الفرد عبر المنصات الرقمية، مثل: سجل التصفح والاستخدام،بيانات الموقع الجغرافي، التفضيلات الشرائية والمحتوى المفضل، نمط التفاعل على وسائل التواصل

وتكتسب هذه البيانات قيمة عالية في خوارزميات الذكاء الاصطناعي لأنها تكشف عن سلوكيات دقيقة تسمح بالتنبؤ بقرارات الفرد وميوله، مما يجعلها أكثر عرضة للاستغلال التجاري أو السياسي.[٢]

ثالثاً: البيانات الحساسة(Sensitive Personal Data)

وهي المعلومات التي يؤدي الكشف عنها إلى انتهاك خطير للحقوق الأساسية، وتشمل:البيانات الصحية والطبية، البيانات الجينية والبيومترية (البصمة – بصمة الوجه – قزحية العين) ، المعتقدات الدينية أو الآراء السياسية، الأصل العرقي أو الإثني.[٣]

وقد منحت التشريعات المقارنة لهذه الفئة حماية مضاعفة نظراً لاستخدامها في أغراض قد تؤدي إلى التمييز أو الإقصاء أو الاعتداء على الحرية الشخصية، خصوصاً في مجالات الائتمان، الأمن، أو التوظيف.

رابعاً: البيانات المستنتجة – (Inferred Data) الأخطر في عصر الذكاء الاصطناعي

وهي المعلومات التي لا يُفصح عنها الفرد مباشرة، بل تستنتجها الخوارزميات عبر تحليل بياناته السلوكية أو الرقمية، مثل:التنبؤ بالحالة الصحية أو النفسية،تحديد

---

(١) د. ايمن الاسيوطي ، نفس المرجع السابق. ص ١٥

(٢) د. زياد عبد التواب ، الذكاء الاصطناعي وتحليل البيانات ، الهيئة المصرية العامة للكتاب ، ٢٠٢١م. ص ٣٢

(٣) كيفن وابل،اساسيات الذكاء الاصطناعي، الهيئة المصرية العامة للكتاب، القاهرة، ٢٠١٣م. ص١٣

الاتجاهات السياسية أو الدينية،تقييم الجدارة الائتمانية أو الخطورة الأمنية، التوقعات السلوكية المستقبلية.[١]

وتتميز هذه البيانات بخطورتها لعدة أسباب:

١. أنها تُنتج دون علم الشخص أو موافقته، مما يقوّض مبدأ الموافقة المستنيرة.
٢. ارتفاع درجة دقتها وتأثيرها القانوني، إذ قد تُستخدم لاتخاذ قرارات مؤتمتة تمس الحقوق الأساسية.
٣. صعوبة تصحيحها أو الاعتراض عليها، لأنها ناتجة عن نماذج تحليلية غير شفافة.

ومن خلال ما تقدّم، يتضح أن حماية البيانات الشخصية في عصر الذكاء الاصطناعي لم تعد مقصورة على المعلومات التي يفصح عنها الفرد طوعاً، بل باتت تقتضي امتداد الحماية لتشمل فئات جديدة من البيانات ذات خطورة متزايدة، وعلى رأسها: البيانات السلوكية التي تُجمع بشكل ضمني دون علم الشخص؛ والبيانات المستنتجة التي تُعد الأخطر لكونها تُولّد خصائص جديدة عن الفرد قد يجهلها هو ذاته؛ والبيانات الحساسة التي قد تُفضي إساءة استخدامها إلى التمييز أو الوصم الاجتماعي؛ إضافة إلى البيانات المدمجة التي تُنتج "ملفاً رقمياً شاملاً" يكشف تفاصيل دقيقة عن حياة الشخص.وفي ضوء ذلك، يصبح جلياً أن الإطار القانوني السوداني في صورته الحالية غير قادر على استيعاب هذا التطور، إذ يخلو من تعريف شامل للبيانات الشخصية، ولا يعترف بالبيانات المستنتجة أو السلوكية أو الحساسة بوصفها فئات مستقلة تتطلب مستويات حماية متدرجة، رغم أنها تمثل جوهر المخاطر التقنية المعاصرة.

ومن ثمّ، تبرز الحاجة إلى أن يتبنى التشريع السوداني المقترح تعريفاً موسعاً ومتدرجاً للبيانات الشخصية، على نحو مماثل للنموذجين الأوروبي والخليجي، بحيث يغطي جميع هذه الفئات، ويضع إطاراً خاصاً لحماية البيانات الحساسة والمستنتجة، باعتبارهما الأكثر تأثيراً على الحقوق والحريات الفردية في بيئة الذكاء الاصطناعي.

الفرع الثاني / مخاطر استخدام البيانات الشخصية في تطبيقات الذكاء الاصطناعي :

أدى توسّع تطبيقات الذكاء الاصطناعي في مختلف القطاعات إلى بروز مجموعة من المخاطر القانونية والأخلاقية المرتبطة باستخدام البيانات الشخصية، لاسيما في ظل

---

(١) د. عبد الله موسى ، د. احمد حبيب بلال ، الذكاء الصناعي ثورة تقنية العصر ، المجموعة العربية للتدريب والنشر ، مصر ، ٢٠١٨م. ص٤٢

قدرته على جمع كميات ضخمة من البيانات، وتحليلها، واستخراج أنماط شديدة الدقة عن الأفراد. وتمتد هذه المخاطر إلى مراحل الجمع والمعالجة والتخزين والاستنتاج واتخاذ القرار، مما يجعل بيانات الأفراد عرضة لاستغلال واسع قد يتجاوز حدود السيطرة التقليدية. ويمكن تلخيص أهم هذه المخاطر في أربعة محاور رئيسية:

أولاً: جمع البيانات دون علم أو موافقة مستنيرة

تعتمد معظم الأنظمة الذكية على أدوات التتبع الخفي (Tracking Tools) وتقنيات جمع البيانات تلقائياً، عبرتتبع السلوك الرقمي للمستخدم؛تسجيل مواقع الأجهزة الجغرافية؛تحليل محتوى المحادثات والتفاعلات؛مراقبة الأنشطة عبر تطبيقات الهاتف.[١]

ويُعدّ هذا النوع من الجمع غير المرئي للبيانات الخطر الأكبر على خصوصية الأفراد، لأنه يتم غالباً دون علمهم أو موافقتهم الصريحة، في انتهاك واضح لمبدأ الموافقة المستنيرة.ويرى الباحثون أن هذا الخطر يتضاعف في السودان بسبب عدم وجود تشريع يفرض على المؤسسات الإفصاح عن طرق جمع البيانات أو يحدد شروط الموافقة وآثارها.

ثانياً: مخاطر التصنيف الآلي والقرارات المؤتمتة

اصبحت أنظمة الذكاء الاصطناعي قادرة على إنشاء ملفات تعريفية دقيقة للأفراد عبر تحليل كميات ضخمة من البيانات، تُستخدم لاحقاً لاتخاذ قرارات ذات أثر قانوني أو اجتماعي مباشر، مثل: قبول أو رفض طلبات التوظيف، تحديد الجدارة الائتمانية، تقدير مستويات الخطورة الأمنية، تصنيف الطلاب والمتقدمين للمنح، وتقييم الأداء الوظيفي.

وتكمن الخطورة في أن هذه القرارات تُتخذ في كثير من الأحيان بشكل مؤتمت بالكامل دون تدخل بشري فعّال، مما يجعلها عرضة للأخطاء التقنية أو الانحيازات الخوارزمية، خصوصاً عندما تعتمد على بيانات غير دقيقة أو غير مكتملة، أو عند استخدام نماذج تحليلية تفتقر إلى الشفافية أو القابلية للتفسير.[٢]

وفي هذا السياق، يبرز القصور التشريعي في السودان بوضوح، إذ لا يتضمن الإطار القانوني الحالي أي نصوص تنظم القرارات الآلية أو تفرض ضرورة المراجعة البشرية للقرارات ذات الأثر الجوهري. ويمثّل هذا الفراغ التشريعي نقطة ضعف أساسية، لأنه يتيح

---

(١) أ. ريان صالح عمر ، الطبيعة القانونية للذكاء الاصطناعي، بحث لاستكمال درجة الماجستير - جامعة بغداد ، العراق ، ٢٠٢٤، ص ٢٥

(٢) أ. ريان صالح عمر ، المرجع السابق ، ص ٣١

استخدام خوارزميات التصنيف والتقييم بطرق قد تؤدي إلى تمييز غير مبرر أو حرمان الأفراد من حقوقهم دون وجود ضمانات قانونية أو آليات اعتراض فعّالة.

ثالثاً: الاستنتاج والتحليل العميق للبيانات الحساسة:

لم تعد قدرات الذكاء الاصطناعي مقتصرة على تحليل البيانات الصريحة التي يفصح عنها الأفراد، بل بات قادراً على استنتاج بيانات شديدة الحساسية انطلاقاً من معطيات قد تبدو في ظاهرها غير حساسة. فبإمكان الأنظمة الذكية، على سبيل المثال، استنتاج الحالة الصحية من أنماط الشراء أو ساعات النوم، وتحديد الميول السياسية من التفاعل الرقمي، ورصد التوجهات الدينية من سلوكيات يومية بسيطة، بل وحتى استنباط الحالة النفسية من نبرة الصوت أو سرعة الكتابة.

وتكمن خطورة هذه الممارسات في أنها تؤدي إلى توليد بيانات لم يفصح عنها الشخص طوعاً، ولم يوافق على جمعها أو معالجتها، وقد لا يدرك وجودها أصلاً. وهو ما يجعل هذه الفئة من البيانات أكثر حساسية من البيانات التقليدية، لأنها تكشف جوانب دقيقة من الحياة الخاصة يمكن أن تُستخدم في أغراض تصنيفية أو استبعادية أو رقابية [1] وفي ضوء ذلك، يبدو واضحاً أن البيانات المستنتجة تتطلب حماية قانونية مشددة، نظراً لآثارها الممتدة على الحقوق الأساسية، خاصة عندما تُوظَّف في نظم اتخاذ القرار المؤتمت أو في تقييم السلوك والجدارة والموثوقية. كما أن تجاهل تنظيمها يؤدي إلى اتساع نطاق التدخل غير المشروع في خصوصية الأفراد وإلى فتح الباب أمام ممارسات قد تُفضي إلى التمييز أو الوصم أو الرقابة ذات الطابع التنبؤي.

رابعاً: الاتجار بالبيانات ونقلها عبر الحدود

أدى التطور التقني المتسارع، في ظل غياب تنظيم قانوني فعّال، إلى نشوء سوق رقمية موازية تُتداول فيها بيانات المستخدمين لأغراض متعددة، تشمل التسويق التجاري، والاستهداف السياسي، والتحليل الأمني، والدعاية الانتخابية، والخدمات الائتمانية. ويعزز هذا الواقع احتمالات إساءة استخدام البيانات على نطاق واسع، سواء من جهات تجارية أو سياسية أو أمنية، في بيئة تغيب عنها معايير الرقابة والشفافية.

---

(١) د. محمود سلامة الشريف ، الطبيعة القانونية للتنبؤ بالجريمة بواسطة الذكاء الاصطناعي ومشروعيته ، دار النهضة العربية ، ٢٠٢٣، ص ٧٧ .

وتتفاقم الخطورة عند نقل البيانات عبر الحدود إلى دول أو جهات لا تتوافر فيها حماية قانونية كافية، إذ تنتقل البيانات إلى أنظمة قانونية أقل صرامة، أو إلى خوادم ومراكز بيانات خارج نطاق السيادة الوطنية، مما يجعلها أكثر عرضة للاختراق أو التسريب أو الاستغلال غير المشروع.[١]

وفي ضوء ذلك، يتبيّن أن غياب قواعد تشريعية واضحة تنظم عمليات نقل البيانات وتحدد متطلبات الحماية عند انتقالها خارج السودان يمثل فجوة قانونية خطيرة ذات آثار عابرة للحدود. فاستمرار هذا الفراغ التشريعي قد يؤدي إلى تعريض خصوصية الأفراد وحقوقهم الأساسية لمخاطر جسيمة، ولا سيما في ظل الاعتماد المتزايد على بنى تحتية رقمية وخدمات سحابية أجنبية.

خامساً: ضعف القدرة على المحو والسيطرة على البيانات:

في البيئة الرقمية المعاصرة تصبح البيانات ذات طبيعة متجددة ومتناسلة؛ فهي قابلة للنسخ اللانهائي، ومحفوظة في خوادم متعددة داخل الدولة وخارجها، وقد تبقى ضمن النسخ الاحتياطية أو مدمجة في نماذج الذكاء الاصطناعي حتى بعد حذفها من المصدر الأصلي. ونتيجة لذلك، يفقد الأفراد القدرة الفعلية على التحكم في بياناتهم أو ضمان محوها بصورة كاملة، رغم طلبهم الصريح بذلك.

ويمثل هذا الواقع تحدياً مباشراً لأحد أهم الحقوق الرقمية الحديثة، وهو الحق في النسيان، الذي يقوم على تمكين الفرد من إزالة بياناته أو منع استمرار استخدامها حين تنتفي الحاجة إليها.[٢]

وفي ضوء ذلك، يبدو من الضروري أن يتضمن التشريع السوداني أحكاماً صريحة تنظم عمليات الحذف، وتحدد مدد الاحتفاظ بالبيانات، وتلزم المؤسسات باتخاذ إجراءات فعلية تضمن الإتلاف التام للبيانات عند انتهاء الغرض الذي جُمعت من أجله، وبما يتوافق مع المعايير الدولية في هذا المجال.

نخلص مما تقدّم عرضه في هذا المطلب- من مخاطر استخدام البيانات الشخصية في تطبيقات الذكاء الاصطناعي - أن التهديدات لا ترتبط بمرحلة بعينها من مراحل المعالجة، بل تمتد لتشمل دورة حياة البيانات بأكملها منذ لحظة جمعها وحتى

---

(١) د. أشرف توفيق شمس الدين، مرجع سابق، ص ٤٢

(٢) د. أشرف توفيق شمس الدين، ص ٤٤

تخزينها واستنتاج خصائص جديدة منها. وتتجلى الخطورة الحقيقية ليس في عملية الجمع المباشر للبيانات فحسب، وإنما في قدرة الأنظمة الذكية على استنباط بيانات لم يصرّح بها الفرد مطلقاً، واتخاذ قرارات مؤتمتة تنتج آثاراً قانونية واجتماعية تمس حقوقه الأساسية. كما تسهم قدرة الذكاء الاصطناعي على دمج البيانات من مصادر متعددة في تكوين ملفات تعريفية شديدة الدقة، تزيد من احتمالات التمييز الخوارزمي أو التقييم غير العادل. ويُضاف إلى ذلك صعوبة ممارسة الأفراد لحقهم في محو البيانات أو التحكم فيها بعد اندماجها في المنصات الرقمية والخوارزميات التحليلية، مما يجعل السيطرة عليها شبه معدومة. وهذه العناصر مجتمعة تؤكد الحاجة الملحّة لإطار قانوني حديث يضمن حماية فعّالة للبيانات الشخصية في بيئة الذكاء الاصطناعي.

وبذلك، يصبح التصدي لهذه المخاطر أمراً ضرورياً، ولا يمكن تحقيقه إلا عبر قانون وطني متخصص يضع قواعد واضحة لمشروعية الجمع والمعالجة والنقل، ويضمن حقوق الأفراد، ويُلزم المؤسسات بمبادئ الموافقة والشفافية والمساءلة.

المبحث الثاني

الإطار القانوني لحماية الخصوصية والبيانات الشخصية في السودان

يُعد الإطار القانوني السوداني لحماية الخصوصية والبيانات الشخصية إطاراً جزئياً وغير مكتمل، يتوزع بين نصوص دستورية عامة وقواعد مدنية وجنائية متفرقة، إضافة إلى أحكام محدودة في قانون مكافحة جرائم المعلوماتية. ورغم أن هذه النصوص تُشكل أساساً أولياً للحماية، إلا أنها لا توفر منظومة قانونية متكاملة تتماشى مع متطلبات العصر الرقمي وتقنيات الذكاء الاصطناعي.

وفي هذا المبحث يتم تناول الإطار القانوني السوداني من خلال مطلبين رئيسيين، الأول يتعلق بالأساس الدستوري والمدني والجنائي لحماية الخصوصية، بينما يحلل المطلب الثاني تنظيم البيانات الشخصية وفق قانون مكافحة جرائم المعلوماتية وتقييم مدى استجابته لمخاطر الذكاء الاصطناعي.

المطلب الأول/ الأساس الدستوري والمدني والجنائي لحماية الخصوصية :

الفرع الأول / الحماية الدستورية والمدنية للخصوصية في السودان :

يمثّل الدستور السوداني الخطوة الأولى في إرساء الحماية القانونية للخصوصية، حيث نصّ دستور جمهورية السودان الانتقالي لسنة ٢٠٠٥ في المادة (٣٧) على أن:

"لكل شخص الحق في الخصوصية، ولا يجوز التدخل في حياته الخاصة أو شؤونه الأسرية أو مراسلاته أو اتصالاته إلا وفقاً للقانون".

ويُعد هذا النص مظلة عامة لحماية حرمة الحياة الخاصة والاتصالات، إلا أنه يظل إطاراً عاماً لا يواكب ما تفرضه البيئة الرقمية المعاصرة من متطلبات تفصيلية، إذ لا يقدم قواعد تنظم كيفية جمع البيانات أو معالجتها أو تخزينها، ولا يقرّ حقوقاً حديثة لصاحب البيانات مثل الحق في التصحيح أو الاعتراض أو النسيان.

أما من الناحية المدنية، فيعتمد القانون السوداني على أحكام المسؤولية التقصيرية الواردة في قانون المعاملات المدنية لسنة ١٩٨٤، ولا سيما المادة (١٣٨) التي نصت على:

"كل فعل سبب ضرراً للغير يلزم مرتكبه بالتعويض ولو كان غير مميز".

ورغم أهمية هذه القاعدة في معالجة الأضرار اللاحقة، إلا أنها تُعد حماية ذات طابع ردعي لاحق وليست حماية وقائية مسبقة، إذ لا تمنع جمع البيانات أو تحليلها دون

إذن، ولا تقدم مفاهيم تشريعية واضحة للبيانات الشخصية أو الحساسة، مما يضعف قدرتها على مواجهة الإشكالات المعقدة التي تثيرها تطبيقات الذكاء الاصطناعي.

وهذه القاعدة، رغم أهميتها، تُعد حماية بعدية (ردعية) وليست وقائية، لأنها تعالج الضرر بعد وقوعه، ولا تمنع جمع البيانات أو تحليلها مسبقاً دون إذن. كما أنها لا توفر تعريفاً تشريعياً للبيانات الشخصية أو الحساسة، مما يحد من قدرة القضاء على تطبيقها في النزاعات المتعلقة بالذكاء الاصطناعي أو المعالجة الآلية للبيانات.

مما تقدم وبالنظر إلى كل هذهالجوانب، يتّضح أن الحماية الدستورية والمدنية الحالية لا تزال تقليدية في بنيتها، ولا تستجيب لطبيعة المخاطر الحديثة المرتبطة بالذكاء الاصطناعي، خاصة في ما يتعلق باستنتاج البيانات الحساسة أو اتخاذ قرارات مؤتمتة تؤثر مباشرة على الأفراد دون وجود ضمانات أو آليات اعتراض واضحة.

الفرع الثاني/ الحماية الجنائية للبيانات الشخصية:

تشكّل النصوص الجنائية أحد أهم أدوات حماية الخصوصية في النظام القانوني السوداني، حيث يجرّم القانون الجنائي لسنة ١٩٩١ جملة من الأفعال التي تمس الحياة الخاصة، مثل التجسس وإفشاء الأسرار والاعتداء على خصوصية الاتصالات.

غير أنّ التنظيم الأكثر ارتباطاً بحماية البيانات الشخصية يظهر في قانون مكافحة جرائم المعلوماتية لسنة ٢٠١٨ وتعديل ٢٠٢٥، ولا سيما المادة (١٧) التي تجرّم الدخول غير المشروع إلى الأنظمة المعلوماتية والاطلاع على البيانات أو نسخها أو تعديلها دون إذن.

كما تضمن القانون نصوصاً تجرم:

- اعتراض الاتصالات الرقمية؛
- نسخ أو نقل البيانات دون موافقة صاحبها؛
- استخدام أدوات تقنية للوصول غير المشروع؛
- نشر الصور والمقاطع والبيانات الخاصة دون إذن.

ورغم أهمية هذه الأحكام في ردع الأفعال التي تستهدف الأنظمة المعلوماتية، إلا أنّ نطاقها - من منظور تحليلي - لا ينصبّ في جوهره على حماية البيانات الشخصية كحق مستقل، وإنما يركز بصورة رئيسية على حماية سلامة الأنظمة التقنية من الاختراق أو الاعتداء. فالتشريع الجنائي لا يتناول مشروعية جمع البيانات أو شروط معالجتها، ولا يتضمن قواعد تتعلق بالموافقة المستنيرة أو ضوابط الاحتفاظ بالبيانات أو

إتلافها، كما لا يتطرق إلى الفئات الحساسة منها أو إلى المخاطر الناشئة عن القرارات المؤتمتة والتصنيف الخوارزمي.

وبناءً على ذلك، تظل الحماية الجنائية في السودان ذات طبيعة عقابية لاحقة أكثر من كونها حماية وقائية تنظيمية، إذ تعالج الفعل بعد وقوعه دون أن تقدم منظومة متكاملة لضبط عمليات جمع البيانات ومعالجتها في بيئة تتزايد فيها تطبيقات الذكاء الاصطناعي وتهديداتها. ومن ثمّ، فإن الاعتماد على النصوص الجنائية وحدها لا يكفي لتوفير حماية فعّالة للبيانات الشخصية، ولا يغني عن الحاجة إلى إطار تشريعي خاص وشامل ينظم دورة حياة البيانات ويوائم بين مقتضيات الابتكار وضمانات الخصوصية.

المطلب الثاني/ تنظيم البيانات الشخصية وفق قانون مكافحة جرائم المعلوماتية وتقييم فعاليته :

الفرع الأول/ نطاق الحماية القانونية في قانون مكافحة جرائم المعلوماتية :

لم يتضمّن قانون مكافحة جرائم المعلوماتية تعريفاً محدداً للبيانات الشخصية، واكتفى بتقديم تعريف عام لمصطلح «البيانات» بوصفها» :كل ما يمكن تخزينه أو معالجته إلكترونياً .«ويُعد هذا التعريف - من منظور تحليلي- تعريفاً محدوداً وغير كافٍ، لعدة اعتبارات جوهرية:

١- **غياب التمييز بين فئات البيانات المختلفة:** لم يميّز القانون بين البيانات الشخصية والبيانات الحساسة مثل الصحية والجينية والبيومترية، ولا بين البيانات المستنتجة الناتجة عن خوارزميات الذكاء الاصطناعي. ويمثل هذا الخلط ضعفاً تشريعياً، لأنه يمنع إسباغ حماية خاصة على الفئات الأكثر خطورة وتأثيراً على الحقوق الأساسية.

٢- **غياب تنظيم دورة حياة البيانات:** يخلو التشريع من أي قواعد تحدد مراحل التعامل مع البيانات بدءاً من جمعها، مروراً بمعالجتها وتخزينها، وانتهاءً بالاحتفاظ أو الإتلاف. وهو عنصر محوري في التشريعات الحديثة، إذ يحدد مسؤولية الجهات المعالجة وضوابط الاستخدام المشروع.

٣- **عدم تنظيم تقنيات الذكاء الاصطناعي:** لم يتناول القانون المخاطر المرتبطة بالمعالجة الخوارزمية أو القرارات المؤتمتة أو التتبع والتحليل العميق للبيانات، ولا يتطرق إلى استنتاج البيانات الحساسة، وهي جميعها مسائل تمثل جوهر التحديات في عصر الذكاء الاصطناعي.

وبناءً على ذلك، فإن نطاق الحماية الذي يقدمه القانون يظل موجهاً بصورة أساسية لحماية الأنظمة المعلوماتية من الاختراق أو العبث، أكثر من كونه إطاراً يضمن حماية

البيانات الشخصية كحق قانوني مستقل .ومن ثمّ، لا يمكن اعتبار هذا القانون بديلاً عن تشريع متكامل لحماية البيانات، بل مجرد جزء من منظومة أوسع ينبغي بناؤها.

الفرع الثاني/ تقييم فعالية الإطار القانوني السوداني في مواجهة الذكاء الاصطناعي:

تكشف الدراسة التحليلية للتشريعات السودانية عن عدد من أوجه القصور البنيوية التي تجعل الإطار القانوني الراهن غير قادر على استيعاب المخاطر المتزايدة المرتبطة بتطبيقات الذكاء الاصطناعي، ويمكن إبراز أهم هذه الإشكالات على النحو الآتي:

١- غياب تشريع وطني متخصص لحماية البيانات:

لا يتوافر في السودان قانون شامل ومنفصل يُعنى بحماية البيانات الشخصية على غرار ما هو معمول به في التجارب الأوروبية والخليجية، وهو ما يؤدي إلى فراغ تشريعي كبير في مجال تنظيم عمليات الجمع والمعالجة والاحتفاظ والنقل.

٢- غلبة المقاربة الأمنية على المقاربة الحقوقية:

تركز التشريعات الحالية – وفي مقدمتها قانون مكافحة جرائم المعلوماتية – على حماية الأنظمة من الاختراق والجريمة الإلكترونية، أكثر من تركيزها على حماية الحقوق الرقمية للأفراد وضمان سيادتهم على بياناتهم. وهذا الخلل في المقاربة يؤدي إلى إضعاف البعد الوقائي والحقوقي.

٣- عدم وجود جهة رقابية مستقلة:

يفتقر السودان إلى مؤسسة وطنية مختصة بحماية البيانات تتولى الرقابة على الجهات المعالجة، وتلقي الشكاوى، وإصدار التراخيص، وفرض الجزاءات. ويمثل غياب هذه الجهة فجوة مؤسسية تحول دون ضمان الامتثال للمعايير القانونية.

٤- عدم مواكبة التشريعات للتطور التقني:

لم تُحدّث المنظومة القانونية لاستيعاب التطبيقات الحديثة للذكاء الاصطناعي، مثل الخوارزميات التنبؤية، والتصنيف المؤتمت، واستنتاج البيانات الحساسة، وقواعد نقل البيانات عبر الحدود. الأمر الذي يجعل النصوص القائمة غير ملائمة لمعالجة المخاطر التقنية المستجدة.

وبناءً على ما سبق، يتضح أن الإطار التشريعي السوداني لا يزال يعتمد على مقاربة عقابية تقليدية تجرّم الأفعال بعد وقوعها، دون توفير نظام تنظيمي ووقائي يضبط عمليات المعالجة ويحمي الأفراد من المخاطر الناجمة عن الأنظمة الذكية. ومن ثمّ، تبدو الحاجة ملحّة لإصدار قانون وطني شامل لحماية البيانات الشخصية يُشكّل قاعدة تشريعية حديثة

قادرة على مواكبة التطور الرقمي المتسارع، خاصة مع اتساع استخدام تقنيات الذكاء الاصطناعي في المؤسسات الحكومية والقطاع الخاص.

المبحث الثالث

نحو إطار قانوني حديث لحماية البيانات في السودان في عصر الذكاء الاصطناعي

تُظهر الدراسة المقارنة للتجارب الدولية - ولا سيما الأوروبية والخليجية - أن حماية البيانات الشخصية في البيئة الرقمية المعاصرة تستلزم وجود إطار تشريعي مستقل ومتخصص، يقوم على مبادئ واضحة وضمانات تقنية وقانونية متكاملة.

وقد أثبتت هذه التجارب أن القوانين التقليدية، وبخاصة قوانين مكافحة الجرائم المعلوماتية، ليست كافية لتوفير الحماية المطلوبة، إذ تركز أساساً على الجوانب العقابية وردع الأنشطة غير المشروعة، دون أن تنظم بصورة شاملة عمليات جمع البيانات ومعالجتها والاحتفاظ بها ونقلها، أو تضبط استخدام الأنظمة الذكية ذات القدرة المتقدمة على الاستنتاج والتحليل.

وانطلاقاً من هذا الواقع، تبدو الحاجة ملحّة في السودان لاعتماد إطار قانوني حديث يستجيب للبيئة الرقمية المتسارعة، ويعالج الثغرات التشريعية القائمة، ويضمن حماية فعالة للخصوصية دون أن يُعيق مسار الابتكار التقني.

ولهذا يتناول هذا المبحث أبرز الاتجاهات التشريعية الرائدة التي يمكن الاستفادة منها، إلى جانب المبادئ القانونية الأساسية الواجب تضمينها في أي تشريع سوداني مقترح، وصولاً إلى بلورة تصور تشريعي متكامل يتناسب مع خصوصية السياق الوطني، وذلك من خلال المطالب الاتية:

المطلب الأول/ الاتجاهات التشريعية المقارنة والاستفادة منها في السياق السوداني:

الفرع الأول / النموذج الأوروبي اللائحة العامة لحماية البيانات GDPR:

تُعدّ اللائحة العامة لحماية البيانات في الاتحاد الأوروبي (GDPR) الإطار التشريعي الأكثر تطوراً واتساعاً على الصعيد الدولي، وقد أرست منظومة معيارية متكاملة تُنظّم حماية البيانات الشخصية وفق رؤية حديثة تستجيب لمتطلبات البيئة الرقمية وتقنيات الذكاء الاصطناعي. وتتميّز اللائحة ببنيتها القانونية المحكمة التي تضبط دورة حياة البيانات بالكامل- من جمعها ومعالجتها وتخزينها، وصولاً إلى إتلافها- مع إحاطة هذه العملية بجملة من المبادئ الجوهرية، من أبرزها: [1]

---

(١) د. ايمن الاسيوطي ، مرجع سابق ، ص ٧٨

١- مبدأ الشرعية وتحديد الغرض:

لا يجوز جمع البيانات أو استخدامها إلا استناداً إلى سبب مشروع ومحدد سلفاً، على نحو يمنع الاستخدامات اللاحقة غير المعلنة أو المخالفة للغرض الأصلي.

٢- مبدأ الشفافية والإفصاح:

تلتزم الجهات المعالجة بإحاطة صاحب البيانات—بأسلوب واضح ومفهوم—بكيفية الجمع، وأغراض الاستخدام، والجهات المتلقية، ومدة الاحتفاظ، والأساس القانوني للمعالجة، بما يعزز حق الفرد في المعرفة والسيطرة.

٣- مبدأ تقليل البيانات:

يحظر على المؤسسات جمع بيانات تتجاوز الحدّ الضروري لتحقيق الغرض المشروع، وهو ما يسهم في الحدّ من الإفراط في المراقبة وتقليص مخاطر المعالجة غير المتناسبة.

٤- منظومة متقدمة لحقوق الأفراد:

تمنح اللائحة صاحب البيانات مجموعة من "الحقوق الرقمية" التي تعزز سيادته على بياناته، وأهمها:حق الوصول والإحاطة،حق التصحيح،الحق في المحو (النسيان)،الحق في تقييد أو الاعتراض على المعالجة،الحق في عدم الخضوع لقرار مؤتمت بالكامل يولّد أثراً قانونياً أو مؤثراً على حياته.

٥- تنظيم القرارات المؤتمتة وبناء الملفات التعريفية(Profiling)

تضع اللائحة قيوداً دقيقة على القرارات الآلية المستندة إلى الذكاء الاصطناعي، ولا تجيز إصدار قرارات ذات أثر قانوني أو جوهري دون تدخل بشري فعّال، مع ضمان حق الفرد في الاعتراض وطلب المراجعة.

٦- إنشاء سلطات وطنية مستقلة لحماية البيانات:

تمثّل هذه السلطات الركيزة الرقابية الأساسية؛ إذ تُعنى بمتابعة الامتثال، واستقبال الشكاوى، وإصدار الغرامات الإدارية، بما يعزز التطبيق الفعلي لأحكام اللائحة.

وفي ضوء ما سبق، يُظهر النموذج الأوروبي أنه يمثل منظومة تشريعية متكاملة تجمع بين حماية قوية للحقوق الرقمية وتمكين الابتكار التقني في آن واحد. كما توفّر اللائحة إطاراً مرجعياً يمكن للسودان الاستفادة منه عند تطوير تشريع وطني حديث قادر

على استيعاب تحديات الذكاء الاصطناعي وضمان المعالجة المسؤولة للبيانات الشخصية ضمن بيئة رقمية آمنة ومنضبطة.

الفرع الثاني/ التجارب الخليجية في حماية البيانات (الإمارات – السعودية – قطر):

شهدت التشريعات الخليجية خلال العقد الأخير تطوراً لافتاً في مجال حماية البيانات الشخصية، مدفوعةً بتسارع التحول الرقمي واتساع الاعتماد على تقنيات الذكاء الاصطناعي في مختلف القطاعات. وتمثل هذه التجارب أهمية خاصة للسودان بالنظر إلى التقارب النسبي في البنية القانونية والإدارية، فضلاً عن اشتراك البيئتين في التحديات المتصلة ببناء منظومات وطنية لحوكمة البيانات.

أولاً: دولة الإمارات العربية المتحدة:

تُعد الإمارات من أكثر الدول العربية تقدّماً في مجال حماية البيانات، إذ أصدرت المرسوم بقانون اتحادي رقم ٤٥ لسنة ٢٠٢١ بشأن حماية البيانات الشخصية، وهو تشريع حديث يستلهم في كثير من أحكامه النموذج الأوروبي .(GDPR) ويتميز بـ:[1]

- تعريفات دقيقة وشاملة للبيانات الشخصية والحساسة، بما يعزز اليقين القانوني ويحدّ من التفسيرات الواسعة.
- تكريس حقوق موسعة لصاحب البيانات، تشمل الحق في الوصول، والتصحيح، والمحو، والاعتراض على القرارات المؤتمتة.
- تنظيم دقيق للمعالجة الخوارزمية، خاصة في المجالات ذات الحساسية العالية مثل الصحة والتمويل.
- استحداث مكتب اتحادي لحماية البيانات يتولى الرقابة والامتثال وتلقي الشكاوى.
- ضوابط صارمة لنقل البيانات عبر الحدود لضمان استمرار الحماية خارج الإقليم القضائي للدولة.

ثانياً/ المملكة العربية السعودية:

شكل نظام حماية البيانات الشخصية لسنة ٢٠٢١ (وتعديل ٢٠٢٣) جزءاً من التحول الرقمي الشامل ضمن رؤية المملكة ٢٠٣٠ .ويتسم بما يلي:[1]

---

(١)أ.د. انس محمد عبد القادر ، المسؤولية المدنية عن اضرار الذكاء الاصطناعي، دار الكتب القانونية ، مصر ، ٢٠٢٤. ص٦٧

- تجريم واضح لسوء استخدام البيانات أو معالجتها دون أساس قانوني معتبر.
- نظام محكم لنقل البيانات عبر الحدود يحافظ على سيادة البيانات الوطنية ويحد من المخاطر العابرة للحدود.
- إلزام المؤسسات بوضع سياسات لحوكمة البيانات تشمل التشفير، الحد الأدنى من الجمع، والتبليغ عن خروقات البيانات خلال مدة محددة.
- اعتماد الموافقة الصريحة والمستنيرة كشرط جوهري لأي معالجة مشروعة.

ثالثاً/ دولة قطر:

تتميز قطر بكونها من أوائل الدول العربية التي سنت تشريعاً خاصاً لحماية البيانات، وذلك بموجب القانون رقم ١٣ لسنة ٢٠١٦. ويتضمن القانون: [٢]

- إطاراً تنظيمياً مؤسسياً فعالاً للرقابة وتلقي الشكاوى عبر وزارة الاتصالات وتكنولوجيا المعلومات.
- معايير واضحة للمعالجة المشروعة تقوم على العدالة والضرورة والتناسب.
- حماية مضاعفة للبيانات الحساسة بما في ذلك البيانات الصحية والبيومترية.
- إلزام الجهات المعالجة بتعيين مسؤول حماية بيانات (DPO) لتطبيق مبادئ الحوكمة الداخلية وتعزيز المساءلة.

مما تقدم ومن خلال استقراء التجارب الخليجية يتضح أن التشريع الفعّال لا ينحصر في الجانب الردعي أو التجريمي، بل يقوم أساساً على نهج وقائي وتنظيمي يضع ضوابط دقيقة للمعالجة، ويضمن وجود هيئة وطنية مستقلة تشرف على الامتثال وتُعزّز حماية الحقوق الرقمية للأفراد. ويمثل هذا الجانب المؤسسي والتنظيمي عنصراً مفقوداً في الإطار القانوني السوداني الراهن، بما يؤكد الحاجة إلى تطوير منظومة حديثة تستلهم أفضل الممارسات الإقليمية والدولية.

---

(١) د. عقدي محمد ، الذكاء الصناعي افاقه ، تطبيقاته ، وابعاده المتعددة عبر الزمان والمكان، مكتبة نور الالكترونية ، ٢٠٢٤م. ص ٥٢

(٢) د. محمود سلامة الشريف ، مرجع سابق ، ص ٥٨

المطلب الثاني / المبادئ القانونية الأساسية الواجب تضمينها في التشريع السوداني المقترح:

الفرع الأول / مبدأ الموافقة المستنيرة والتحكم في البيانات:

يُعد مبدأ الموافقة المستنيرة الركيزة الأساسية لأي إطار تشريعي حديث لحماية البيانات الشخصية، إذ يُجسّد سيادة الفرد على بياناته ويمثل خط الدفاع الأول ضد المعالجة التعسفية أو غير المشروعة. ويقتضي هذا المبدأ أن تكون الموافقة: [١]

- صريحة : بمعنى واضحة لا يشوبها لبس أو غموض.
- مسبقة: أي تُمنح قبل الشروع في جمع البيانات أو معالجته.
- حرة : تصدر دون ضغط أو إكراه مباشر أو غير مباشر.
- مستنيرة:مبنية على معرفة كاملة بطبيعة البيانات والغرض من معالجتها وآثارها المحتملة.
- قابلة للسحب :بحيث يجوز لصاحب البيانات الرجوع عنها في أي وقت دون أن يترتب على ذلك أي انتقاص من حقوقه أو خدماته.

ويلاحظ أن غياب هذا المبدأ في الإطار القانوني السوداني الحالي يمثل أحد أبرز الاختلالات التشريعية، إذ يتم جمع البيانات ومعالجتها في مؤسسات حكومية وخاصة دون إعلام الأفراد بكيفية استخدامها، أو الأغراض التي جُمعت من أجلها، أو الجهات التي قد تُشارك معها. كما لا تُتاح للأفراد آليات تمكّنهم من إدارة موافقتهم أو سحبها بصورة فعالة.

ويمتد نطاق هذا المبدأ ليشمل مجموعة من الحقوق المتفرعة التي تُعد مكملة له، من أبرزها: [٢]

- حق الاعتراض على المعالجة إذا كانت تضرّ بمصالح الفرد أو تمس خصوصيته.
- حق تقييد استخدام البيانات في ظروف معينة، خاصة عند وجود نزاع حول دقتها أو مشروعيتها.
- حق سحب الموافقة في أي مرحلة من مراحل المعالجة.
- حق منع إخضاع الفرد لقرارات مؤتمتة بالكامل تعتمد على الخوارزميات دون تدخل بشري، خصوصاً عندما تنتج عنها آثار قانونية أو اجتماعية ملموسة.

ومن منظور تحليلي، يُعد تضمين هذا المبدأ في التشريع السوداني المقترح شرطاً أساسياً لضمان العدالة الرقمية وتعزيز الثقة في البيئة التقنية، فضلاً عن كونه متطلباً

---

(١) د. ايمن الاسيوطي ، مرجع سابق ، ص ٨١

(٢)أ. ريان صالح عمر ، مرجع سابق ، ص ٦٣

جوهرياً للمواءمة مع المعايير الدولية وأفضل الممارسات المقارنة في مجال حماية البيانات الشخصية.

الفرع الثاني/ مبدأ الشفافية والمساءلة وأمن البيانات:

تُمثّل مبادئ الشفافية والمساءلة وأمن البيانات ركائز أساسية لأي إطار تشريعي حديث لحماية البيانات الشخصية، لاسيما في ظل التوسع المتزايد في استخدام تقنيات الذكاء الاصطناعي التي تقوم على جمع وتحليل ومعالجة كمّ هائل من البيانات. وتتكامل هذه المبادئ فيما بينها لضمان معالجة منضبطة ومشروعة للبيانات، وتوفير بيئة رقمية تسودها الثقة والوضوح.

أولاً: مبدأ الشفافية:

يُعد مبدأ الشفافية أحد أهم الضمانات التي تمكّن الأفراد من ممارسة سيادتهم على بياناتهم الشخصية، إذ يفرض على الجهات المعالجة التزاماً بالإفصاح الواضح عن جميع مراحل جمع البيانات واستخدامها. ويتضمن هذا المبدأ بوجه خاص: [١]

- بيان طبيعة البيانات التي يتم جمعها والأغراض المحددة لمعالجتها؛
- الإفصاح عن الجهات التي قد تُنقل أو تُشارك معها البيانات، سواء داخل السودان أو خارجه؛
- تحديد مدة الاحتفاظ بالبيانات والمعايير التي تُستند إليها في تحديد هذه المدة؛
- إعلام الأفراد باستخدام الأنظمة الخوارزمية أو تقنيات الذكاء الاصطناعي في اتخاذ القرارات، ولاسيما القرارات ذات الأثر القانوني أو الاجتماعي المباشر.

ويُعد تعزيز الشفافية شرطاً جوهرياً لترسيخ الثقة الرقمية، إذ إن غيابها يؤدي إلى انتشار ممارسات معالجة خفية للبيانات، ويجعل الأفراد عرضة للتصنيف الخوارزمي دون علم أو موافقة، بما يمس جوهر الحق في الخصوصية.

ثانياً/ مبدأ المساءلة:

يقوم مبدأ المساءلة على تحميل الجهة المعالجة مسؤولية قانونية كاملة عن سلامة عمليات جمع البيانات ومعالجتها، سواء تمت بواسطة المؤسسة نفسها أو عبر أطراف أخرى. ويتجسد هذا المبدأ في التزامات عدة، أبرزها: [٢]

- توثيق كافة عمليات المعالجة وإتاحتها للجهات الرقابية المختصة عند الطلب؛

---

(١) د. محمود سلامة الشريف ، مرجع سابق ، ص ٨٣

(٢) د. ايمن الاسيوطي ، مرجع سابق ، ص ٨٥

- تعيين مسؤول حماية بيانات (DPO) يتولى الإشراف على الامتثال القانوني وإدارة المخاطر المرتبطة بالمعالجة؛
- إجراء تقييمات أثر المعالجة(DPIA) ، لاسيما في الأنشطة التي تستخدم الذكاء الاصطناعي عالي الخطورة، بهدف تحديد احتمالات المساس بالحقوق ووضع الضمانات الملائمة.

ويسهم ترسيخ هذا المبدأ في بناء منظومة حوكمة رقمية فعّالة داخل المؤسسات العامة والخاصة، ويُعد خطوة أساسية لضبط القرارات المؤتمتة التي قد تُحدث آثاراً جوهرية على الأفراد.

ثالثاً / مبدأ أمن البيانات:

يمثل أمن البيانات حجر الزاوية في حماية الخصوصية الرقمية، إذ يقتضي اتخاذ تدابير تقنية وتنظيمية فعّالة للوقاية من الوصول غير المشروع أو الاختراق أو التسريب. ويتضمن هذا المبدأ: [1]

- اعتماد تقنيات تشفير قوية لحماية البيانات أثناء التخزين والنقل؛
- وضع ضوابط تحقق دقيقة تمنع الوصول غير المصرح به؛
- تأمين البنية التحتية وقواعد البيانات وفق معايير الأمن السيبراني الدولية؛
- الالتزام بالإبلاغ الإلزامي عن خروقات البيانات خلال فترة زمنية محددة، بما يسمح بالحد من الأضرار ومعالجتها دون تأخير.

مما تقدم ، يتّضح أن مبادئ الشفافية والمساءلة وأمن البيانات تشكّل الحد الأدنى لأي إطار قانوني متين لحماية البيانات، وأن غيابها في المنظومة التشريعية السودانية الحالية يترك فجوات واسعة تتيح معالجة البيانات ـ بما في ذلك البيانات الحساسة والمستنتجة ـ دون ضوابط فعالة. ومن ثمّ، فإن إدماج هذه المبادئ ضمن التشريع السوداني المقترح يُعد ضرورة تشريعية لضبط استخدام الذكاء الاصطناعي وضمان ألا تُستخدم البيانات بطريقة تضرّ بالأفراد أو تُقوّض الثقة في البيئة الرقمية.

---

(١) أ . ريان صالح عمر ، مرجع سابق ، ص ٦٧

الخاتمة:

تُظهر هذه الدراسة أن حماية الخصوصية والبيانات الشخصية في ظل التطور المتسارع لتقنيات الذكاء الاصطناعي أصبحت من أبرز التحديات القانونية المعاصرة، لما تنطوي عليه هذه التقنيات من توسّع كبير في جمع البيانات ومعالجتها واستنتاج أنماط دقيقة قد تمس جوهر الحقوق والحريات الأساسية. وقد بيّن التحليل أن الذكاء الاصطناعي، رغم إسهامه في تحسين كفاءة الخدمات وتعزيز الأداء المؤسسي، يفرز مخاطر حقيقية على الخصوصية متى ما استُخدم في غياب إطار قانوني منظم يحدد ضوابط المعالجة ومسؤوليات الجهات القائمة عليها.

وبناءً على ما تقدم، تنتهي الدراسة إلى مجموعة من النتائج والتوصيات التي تمثل خارطة طريق لتطوير الإطار القانوني السوداني في مجال حماية الخصوصية والبيانات الشخصية، وذلك على النحو الآتي:

أولاً/ النتائج:

١. يتضح من الدراسة أن السودان يفتقر إلى قانون ينظم حماية البيانات الشخصية، الأمر الذي يجعل منظومة الحماية القانونية مجزأة وغير قادرة على مواجهة التحديات المعقدة التي تطرحها تقنيات الذكاء الاصطناعي.

٢. قانون مكافحة جرائم المعلوماتية، بصيغته الحالية، يعتريه قصور بشأن حماية البيانات الشخصية، لأنه يركز على حماية الأنظمة من الاختراق والاعتداءات الإلكترونية، دون تنظيم لحقوق صاحب البيانات أو مراحل جمعها ومعالجتها.

٣. غياب تعريفات قانونية دقيقة لفئات البيانات المختلفة كالبينات الحساسة، البيومترية، والسلوكية والمستنتجة، مما يؤدي إلى تضييق نطاق الحماية القانونية ويُحدث تفاوتاً في التطبيق القضائي.

٤. عدم وجود تنظيم قانوني للقرارات المبنية على الذكاء الاصطناعي، رغم انتشار استخدامها في مجالات تمس الحقوق الأساسية مثل التعليم، التوظيف، الائتمان والتمويل، مما يفتح الباب أمام مخاطر التحيز والتمييز الخوارزمي.

٥. عدم وجود جهة وطنية مختصة بحماية البيانات يؤثر سلباً في الرقابة المؤسسية، ويجعل الجهات المعالجة للبيانات- الحكومية والخاصة- بعيدة عن أي مساءلة فعلية أو إشراف تقني وقانوني.

٦. توسع استخدام الأنظمة الذكية في السودان دون التزام بقواعد الشفافية والمساءلة، ما يزيد احتمالات تسريب البيانات أو إساءة استخدامها أو توظيفها في عمليات تصنيف آلي تؤثر على حقوق الأفراد وحرياتهم.

ثانياً / التوصيات:

١. سنّ قانون سوداني شامل لحماية البيانات الشخصية، مستقل عن قوانين مكافحة الجرائم المعلوماتية، يتضمن تنظيماً كاملاً لدورة حياة البيانات منذ جمعها وحتى إتلافها.

٢. وضع تعريفات قانونية دقيقة ومتفق عليها لأنواع البيانات، تشمل: البيانات الشخصية، الحساسة، البيومترية، السلوكية، والمستنتجة، إلى جانب تحديد مفهوم المعالجة الإلكترونية وضوابطها.

٣. إنشاء هيئة وطنية مستقلة لحماية البيانات تتمتع بصلاحيات تنظيمية ورقابية، وتختص بتلقي الشكاوى، إصدار التوجيهات، وفرض الجزاءات على المخالفين، على غرار الهيئات المعمول بها في الأنظمة المقارنة.

٤. تكريس مجموعة من الحقوق الرقمية الأساسية للأفراد، أبرزها الحق في الإخطار والمعرفة، الحق في الوصول، التصحيح، الحق في المحو (النسيان)، الحق في الاعتراض، الحق في عدم الخضوع لقرارات مؤتمتة بالكامل.

٥. فرض التزامات واضحة ومشددة على المؤسسات التي تعالج البيانات تتعلق بالتشفير، ومعايير الأمن السيبراني، ومبدأ الحد الأدنى من جمع البيانات، وواجب الإبلاغ عن خروقات البيانات خلال فترة زمنية محددة.

المصادر والمراجع :

١- د. أشرف توفيق شمس الدين، الذكاء الاصطناعي والمسؤولية القانونية، دار النهضة العربية، ٢٠٢١.

٢- . د. عبد الفتاح بيومي حجازي، الحماية القانونية للبيانات في البيئة الرقمية، القاهرة، ٢٠٢٠.

٣- د. سامي بشارة، "حماية الخصوصية في البيئة الرقمية"، المجلة العربية للقانون، العدد ٤، ٢٠٢١.

٤- إيمان عبد الله، "الحق في الخصوصية في ظل الذكاء الاصطناعي"، مجلة الحقوق، جامعة القاهرة، ٢٠٢٢.

٥- د. منال البلقاسي، الذكاء الصناعي – صناعة المستقبل (الحاسبات المتوازية – التحكم الالي – البرمجة الوراثية – لغة البرولوج – الخلايا العصبية)، مكتبة نور الالكترونية ، ٢٠٢٤.

٦- د. قصي حبيب ، مقدمة في الشبكات العصبية الاصطناعية ، جامعة صلاح الدين ، كردستان العراق ، ٢٠٢١

٧- د. ايمن الاسيوطي ، الجوانب القانونية لتطبيق الذكاء الاصطناعي، دار النهضة العربية، ٢٠٢٤.

٨- أ. ريان صالح عمر ، الطبيعة القانونية للذكاء الاصطناعي، بحث لاستكمال درجة الماجستير - جامعة بغداد ، العراق ، ٢٠٢٤.

٩- د. محمود سلامة الشريف ، الطبيعة القانونية للتنبؤ بالجريمة بواسطة الذكاء الاصطناعي ومشروعيته ، دار النهضة العربية ، ٢٠٢٣.

١٠- د. محمود طارق هارون ، مدخل الى علم الذكاء الاصطناعي ، دار النشر العربية ، القاهرة ، ٢٠١٩.

١١- أ . حسام حسن ، تاريخ الذكاء الاصطناعي ، دار النهضة العربية ، ٢٠١٢م.

١٢- د. زياد عبد التواب ، الذكاء الاصطناعي وتحليل البيانات ، الهيئة المصرية العامة للكتاب ، ٢٠٢١م.

١٣- د. عقدي محمد ، الذكاء الصناعي افاقه ، تطبيقاته ، وابعاده المتعددة عبر الزمان والمكان، مكتبة نور الالكترونية ، ٢٠٢٤م.

١٤- أ.د. انس محمد عبد القادر ، المسؤولية المدنية عن اضرار الذكاء الاصطناعي، دار الكتب القانونية ، مصر ، ٢٠٢٤.

١٥- كيفن وابل ،اساسيات الذكاء الاصطناعي ، الهيئة المصرية العامة للكتاب ، القاهرة ، ٢٠١٣م.

١٦- د. عبد الله موسى ، د. احمد حبيب بلال ، الذكاء الصناعي ثورة تقنية العصر ، المجموعة العربية للتدريب والنشر ، مصر ، ٢٠١٨م.