التحديات التي يطرحها الذكاء الاصطناعي على الحقوق والحريات: أية ضمانات قانونية لمواجهة مخاطر التمييز والمس بالخصوصية ؟

مصطفى اهدار
طالب باحث بسلك الدكتوراه، بكلية العلوم القانونية والاقتصادية والاجتماعية بأيت ملول، جامعة ابن زهر المغرب

■ **ملخص**

شهدت السنوات الأخيرة تطورا متسارعا في تقنيات الذكاء الاصطناعي، مما أتاح فرصا هائلة لتعزيز الرفاه والتنمية. غير أن هذا التطور التقني صاحبته تحديات عميقة تمس الحقوق والحريات الأساسية للأفراد، وعلى رأسها الحق في الخصوصية ومبدأ عدم التمييز. يسلط هذا البحث الضوء على الإشكالات القانونية الناشئة عن استخدامات الذكاء الاصطناعي والتي قد تؤدي إلى انتهاك خصوصيات الأفراد عبر جمع وتحليل كميات غير مسبوقة من البيانات الشخصية، أو إلى ممارسات تمييزية ناتجة عن التحيز الخوارزمي في خوارزميات صنع القرار الآلي. ومن خلال منهج تحليلي حجاجي، يتناول البحث مفهوم الحق في الخصوصية في العصر الرقمي ومدى تأثره بالتقنيات الذكية، مع استعراض الأطر القانونية الوطنية والدولية التي تسعى لحمايته، لا سيما في التشريع المغربي والنموذج الأوروبي (خاصة النظام العام لحماية البيانات GDPR). كما يناقش البحث مخاطر التحيز والتمييز الناتج عن خوارزميات الذكاء الاصطناعي، مبرزا الثغرات القانونية في مواجهتها والحاجة إلى ضمانات تكفل المساواة وعدم التمييز. ويقدم البحث مقارنة قانونية بين المقاربة المغربية ونظيرتها الأوروبية، من حيث التشريعات والضمانات المتاحة، كاشفا عن مواطن التقارب والتباين بينهما. ويخلص إلى جملة من الاستنتاجات والتوصيات العلمية، أبرزها ضرورة تطوير إطار قانوني متكامل ومرن لمواكبة التطور التقني السريع، يضمن حماية الحياة الخاصة للأفراد ويكافح التمييز الخوارزمي، عبر آليات مثل إلزامية تقييم الأثر على الخصوصية وضمان شفافية الخوارزميات وخضوعها للمساءلة. بذلك يسعى البحث للإجابة عن التساؤل المحوري :أي ضمانات قانونية كفيلة بدرء مخاطر الذكاء الاصطناعي على الحقوق والحريات الأساسية في المجتمع المعاصر؟

- **Abstract**

In recent years, the rapid advancement of artificial intelligence (AI) technologies has created tremendous opportunities for improving welfare and development. However, this technological progress has been accompanied by profound challenges to fundamental rights and freedoms, foremost among them the right to privacy and the principle of non-discrimination. This research sheds light on the legal issues arising from the use of AI that may lead to privacy infringements through the unprecedented collection and analysis of personal data, or result in discriminatory practices stemming from algorithmic bias in automated decision-making systems. Through an analytical and argumentative methodology, the paper examines the concept of the right to privacy in the digital age and how it is affected by intelligent technologies, reviewing national and international legal frameworks aimed at its protection – particularly in Moroccan legislation and the European model (especially the GDPR). It also discusses the risks of bias and discrimination produced by AI algorithms, highlighting legal gaps in addressing them and the need for safeguards to ensure equality and non-discrimination. The research presents a comparative legal analysis between the Moroccan approach and its European counterpart in terms of legislation and available safeguards, revealing points of convergence and divergence. It concludes with a set of scientific conclusions and recommendations, most notably the necessity of developing a comprehensive and flexible legal framework to keep pace with rapid technological development, one that guarantees the protection of individuals' private life and combats algorithmic discrimination. Such a framework would include mechanisms like mandatory privacy impact assessments, ensuring algorithmic transparency, and accountability. The study thus seeks to answer the central question: *What legal safeguards can counter the risks that AI poses to fundamental rights and freedoms in contemporary society?*

- **مقدمة منهجية**

لا يخفى أن التطورات المذهلة في مجال الذكاء الاصطناعي قد أدخلت البشرية عصرا جديدا يزخر بالفرص والتحديات في آن واحد. فمن جهة، تعد تقنيات الذكاء الاصطناعي بإمكانات هائلة لتحسين حياة الإنسان في ميادين شتى، كالرعاية الصحية والنقل والتعليم وتحليل البيانات الضخمة، كما أنها تساهم في اتخاذ قرارات أكثر فعالية وابتكار حلول للمشكلات المعقدة. ومن جهة أخرى، يثير الانتشار المتزايد لهذه التقنيات الذكية مخاوف جدية بشأن الحقوق والحريات الأساسية للأفراد، إذ باتت قدرات الذكاء الاصطناعي على جمع المعلومات وتحليلها واتخاذ القرارات تتمدد إلى مجالات تمس جوهر كرامة الإنسان وحرمته. وفي هذا السياق برز تساؤل ملح في الأوساط القانونية والحقوقية مفاده : **هل الإطار القانوني القائم كاف لضمان ألا تتحول تقنيات الذكاء الاصطناعي إلى أدوات لانتهاك الخصوصية أو التمييز بين الأفراد؟**

إن الحق في الخصوصية – بمعناه العام وفي بعده المتعلق بحماية الحياة الخاصة والمعطيات الشخصية – يواجه اليوم تحديات غير مسبوقة بفعل تقنيات الذكاء الاصطناعي القائمة على البيانات الضخمة والتعلم الآلي. فهذه التقنيات قادرة على التتبع الدقيق لأنشطة الأفراد وتجميع تفاصيل حميمة عن حياتهم وتفضيلاتهم وحتى تنبؤ سلوكياتهم المستقبلية، وذلك من خلال تحليل أنماط البيانات والاعتماد على الخوارزميات المتقدمة. وهكذا أضحى انتهاك الخصوصية خطرًا حقيقيًا إذا لم توجد ضوابط تحكم جمع البيانات الشخصية واستعمالها. بالموازاة، يتنامى القلق من أن تؤدي الأنظمة الذكية – عن قصد أو غير قصد – إلى تكريس أنماط من التمييز بين الأشخاص أو الفئات، وذلك عندما تعكس الخوارزميات تحيزات ضمنية في البيانات التي درّبت عليها أو في تصميمها ذاته. وعليه فإن مبدأ المساواة وعدم التمييز – وهو من صميم الحقوق الإنسانية – قد يتعرض للمساس إذا لم توضع ضمانات تكفل عدالة مخرجات أنظمة الذكاء الاصطناعي وحياديتها.

من الناحية القانونية، يطرح ما سبق إشكالات معقدة أمام المشرّعين والقضاء على حد سواء. فالقوانين التقليدية الموضوعة لحماية الحقوق – كحماية الحياة الخاصة أو منع التمييز العنصري أو الجنسي وغيرها – وضعت في زمن سابق على هذه التقنيات، وقد لا تسعف نصوصها الحالية في التصدي للتحديات المستجدة. لذلك غدت مسألة تحديث المنظومة القانونية أمرا ضروريا لإيجاد توازن بين متطلبات الابتكار التقني من جهة، وضمان احترام الحقوق والحريات الجوهرية من جهة أخرى. وفي هذا الإطار، اتخذت بعض التجارب الدولية خطوات سباقة، يأتي في مقدمتها النموذج الأوروبي بإقرار اللائحة العامة لحماية البيانات (GDPR) وما تضمنته من مبادئ صارمة لحماية المعطيات الشخصية[1]. كما برزت توجهات لإصدار قوانين خاصة بالذكاء الاصطناعي – كالمقترح الجاري دراسته في المغرب لتنظيم هذه التقنية[2] – إدراكا للحاجة الملحة لإطار تنظيمي محين ومتكامل.

بناء على ما تقدم، تنصب إشكالية هذا البحث على تحليل التحديات القانونية التي يطرحها الذكاء الاصطناعي على الحق في الخصوصية والحماية من التمييز، واستقصاء الضمانات القانونية الممكنة لمواجهة مخاطر المساس بهذين الحقين. وسيتخذ البحث منهجا تحليليا حجاجيا يستند إلى دراسة النصوص التشريعية الوطنية والدولية ذات الصلة، وإلى أدبيات فقه القانون وتقارير الهيئات الرسمية. وفي سبيل معالجة الموضوع، سيتم تقسيم الدراسة إلى محاور رئيسية تعالج تباعا: المحور الأول: التأصيل المفاهيمي والقانوني للحق في الخصوصية في ظل الذكاء الاصطناعي، مع بيان التهديدات التي تتعرض لها الخصوصية نتيجة الاستخدامات الحديثة لهذه التقنية؛ المحور الثاني: تحليل التحديات المتعلقة بالتمييز والتحيز في سياق الذكاء الاصطناعي، وبيان أوجه القصور القانوني في منع التمييز الخوارزمي؛ المحور الثالث: إجراء مقارنة قانونية بين التشريع المغربي والنموذج القانوني الأوروبي في التعامل مع مسألتي حماية الخصوصية ومكافحة التمييز في سياق الذكاء الاصطناعي، مع التركيز على حالة اللائحة الأوروبية العامة لحماية البيانات (GDPR) وما يقابلها في المنظومة المغربية؛ وأخيرا خاتمة تتضمن أهم الاستنتاجات والتوصيات العملية المستخلصة من البحث. بذلك يأمل البحث في الإسهام بسد فجوة معرفية حول موضوع حديث وحيوي، ويوجه النظر نحو ضرورة تبني مقاربة قانونية استباقية تكفل تسخير الذكاء الاصطناعي لخدمة المجتمع دون التفريط بقيمه الدستورية وحقوق أفراده الأساسية.

أولًا: الحق في الخصوصية في ظل الذكاء الاصطناعي – تحليل قانوني

1. تحديد المفاهيم وأهمية الحق في الخصوصية

الخصوصية في سياق القانون هي حق الفرد في حماية حياته الخاصة وعدم إفشاء أسراره الشخصية ومعطياته الحساسة بدون رضاه. وقد اكتسب هذا الحق بعدًا عالميًا باعتباره حقا أساسيا من حقوق الإنسان؛ حيث نصت المواثيق الدولية على ضمان احترام الحياة الخاصة للأفراد وعدم التعرض التعسفي لخصوصياتهم (كما في المادة 12 من الإعلان العالمي لحقوق الإنسان والمادة 17 من العهد الدولي للحقوق المدنية والسياسية)[3]. وعلى الصعيد الدستوري الوطني، أكد دستور المملكة المغربية لسنة 2011 صراحة على حماية خصوصية الأفراد، حيث جاء في الفصل 24 منه أن" لكل شخص الحق في حماية حياته الخاصة .ولا تنتهك حرمة المنزل... ولا تنتهك سرية الاتصالات الشخصية بكل أشكالها إلا بأمر قضائي وفق الشروط والإجراءات التي ينص عليها القانون"[4]. يتضح من ذلك أن المشرع الدستوري أضفى حرمة خاصة على الحياة الخاصة والمعطيات الشخصية واعتبرها خطا أحمر لا يجوز المساس به إلا وفق ضمانات قانونية وضوابط قضائية صارمة.

تنبع أهمية الحق في الخصوصية من كونه حجر الزاوية لضمان كرامة الإنسان واستقلاليته .فالقدرة على التحكم في معلوماتنا الشخصية وحرية اتخاذ قرار بشأن مشاركتها تعد شرطا أساسيا لتمتعنا بحرياتنا الأخرى كالحرية الفكرية وحرية التعبير. وقد أكدت اليونسكو في توصياتها بشأن أخلاقيات الذكاء الاصطناعي (2021) هذا المعنى[5]، حيث اعتبرت الخصوصية حقا جوهريا لصون الكرامة الإنسانية وحرية الفرد، ينبغي حمايته في جميع مراحل دورة حياة أنظمة الذكاء الاصطناعي. ومن هذا المنطلق، تغدو حماية الخصوصية مسؤولية قانونية وأخلاقية ملقاة على عاتق الدول والشركات على السواء في خضم الثورة الرقمية الراهنة.

2. تأثيرات تقنيات الذكاء الاصطناعي على الحق في الخصوصية

أدت تقنيات الذكاء الاصطناعي القائمة على خوارزميات التعلم الآلي ومعالجة البيانات الضخمة إلى تغيير جذري في مشهد الخصوصية. فهذه التقنيات قادرة على جمع وتخزين وتحليل كميات هائلة من البيانات الشخصية عن الأفراد، تشمل كل ما يصدر عنهم من أثر رقمي في حياتهم اليومية – من بيانات التصفح على الإنترنت والتفاعلات عبر وسائل التواصل الاجتماعي إلى بيانات المواقع الجغرافية وأنماط الاستهلاك والسجل الصحي والبيومتري. ولا يقتصر الأمر على البيانات التي يفصح عنها الفرد طواعية، بل يمتد ليشمل بيانات يتم استنتاجها أو تنبؤها بواسطة الخوارزميات دون علمه أو فهمه. وقد أشارت مفوضية الأمم المتحدة لحقوق الإنسان إلى أن أنظمة الذكاء الاصطناعي تعتمد على مجموعات بيانات ضخمة، تُجمع وتُدمج وتُحلل بطرق معقدة وغير شفافة، مما يجعل انتهاك الخصوصية خطرا قائما ما لم تتخذ إجراءات صارمة لحماية البيانات[6]. على سبيل المثال، تتيح خوارزميات التعرف على الوجوه تتبع تحركات الأفراد في الفضاء العام بشكل لحظي، كما تسمح تقنيات تحليل البيانات بتكوين صورة دقيقة عن سمات الشخص وتوجهاته قد تستخدم لأغراض تجارية أو سياسية دون رضاه.

إن أخطر ما في الأمر هو غموض الطريقة التي تعمل بها الخوارزميات وصعوبة إدراك الأفراد لحجم البيانات التي تُجمع عنهم وكيفية استخدامها. فكثيرا ما تعمل تقنيات الذكاء الاصطناعي في الخفاء، ولا يشعر الفرد بأنه مراقب أو أنه موضع تحليل لخوارزمية ما. وهذا يحد من قدرة الناس على اتخاذ قرارات واعية بشأن حماية حياتهم الخاصة. ومن مظاهر ذلك انتشار التطبيقات والخدمات الرقمية التي تجمع البيانات بطرق تتجاوز نطاق الغرض المعلن، أو مشاركة البيانات مع أطراف ثالثة دون إفصاح واضح. وعندما تقترن هذه الممارسات بقدرات الذكاء الاصطناعي في الاستدلال والاستنتاج، يمكن أن تتوصل الأنظمة لتحليلات عميقة حول سلوك الفرد وشخصيته (مثل توقع الحالة الصحية أو المستوى الاقتصادي أو حتى المعتقدات) من مجرد أنماط سلوكية في البيانات. وهذا يمثل انتهاكًا مضمرًا للخصوصية يفوق بكثير الانتهاكات التقليدية المحدودة النطاق.

في ظل هذه المعطيات، صار هاجس حماية الخصوصية digital privacy هاجسًا عالميًا دفعت إليه فضائح متتالية تتعلق بإساءة استخدام البيانات. ولعل من أبرز الأمثلة على ذلك قضية *شركة "كامبريدج أناليتكا"* عام 2018، حيث استغلت بيانات الملايين من مستخدمي فيسبوك لتحليل توجهاتهم والتأثير على خياراتهم السياسية دون علمهم، مما أثار زوبعة من التساؤلات حول مدى كفاية القوانين في ردع مثل هذه الممارسات[7]. كذلك برزت مخاطر *المراقبة الجماعية* عبر الذكاء الاصطناعي، كما في استخدام تقنيات التعرف على الوجه من طرف بعض الأجهزة الأمنية، الأمر الذي دفع جهات حقوقية للمطالبة بفرض حظر أو قيود على هذه التطبيقات لحين وضع قواعد تنظيمية واضحة تحمي الخصوصية. إن هذه الأمثلة وغيرها تدل على أن الذكاء الاصطناعي قد يصبح – إذا غابت الضوابط – أداة لانتهاك الحياة الخاصة على نطاق واسع، عبر ما يُعرف بـ"الانتهاك الصامت" الذي لا يدركه الضحايا إلا بعد فوات الأوان[8].

3. الأطر القانونية لحماية الخصوصية في سياق الذكاء الاصطناعي

أمام هذه التحديات، برزت استجابات قانونية على المستوى الدولي والإقليمي تهدف إلى تعزيز حماية الخصوصية في العصر الرقمي. ويأتي في مقدمة هذه الاستجابات النظام القانوني الأوروبي الذي يعد رائدا في إرساء معايير صارمة لحماية البيانات الشخصية. فقد اعتمد الاتحاد الأوروبي عام 2016 اللائحة العامة لحماية البيانات (GDPR) التي دخلت حيز التنفيذ سنة 2018، لتحل محل توجيه 1995. وتتميز الـ GDPRبأنها وضعت *إطارا قانونيا حديثا* يواكب التطور التكنولوجي، حيث تفرض على الجهات التي تعالج البيانات الشخصية التزامات صارمة، من بينها: الحصول على موافقة صريحة ومسبقة من الشخص المعني قبل جمع بياناته إلا في حالات قانونية محددة، واعتماد مبدأ الغرض المحدد (أي عدم جمع البيانات إلا لأغراض مشروعة ومعلنة)، ومبدأ تقليل البيانات)ألا تجمع إلا البيانات الضرورية فقط – وهو ما يسمى مبدأ حصر المعطيات أو (data minimization الذي لم يكن موجودا في القانون المغربي وقت صدوره، بالإضافة إلى *حقوق جديدة للمواطنين* منها حق النسيان (أي حق الشخص في محو بياناته لدى الغير) وحق قابلية نقل البيانات من منصة إلى أخرى، وحق الحصول على نسخة من البيانات والاعتراض على بعض المعالجات الآلية. كما ألزمت اللائحة الأوروبية المؤسسات بإخطار سلطات حماية البيانات وأصحاب البيانات بأي خرق أمني أو تسرب بيانات في غضون 72 ساعة من اكتشافه، وهو ما يعرف بالتبليغ الإجباري عن خروقات البيانات – وهذا أيضا عنصر غائب في التشريع المغربي الحالي. وعلاوة على ما سبق، خصت الـ GDPRمعالجة البيانات ذات الطابع الشخصي بتدابير خاصة عندما يتعلق الأمر بالاستعمالات التقنيات الحديثة؛ فالمادة 22 منها منحت الأفراد حقا في عدم الخضوع لقرار مبني بشكل أحادي على معالجة آلية (كخوارزمية ذكاء اصطناعي) إذا كان لهذا القرار أثر قانوني أو جوهري على حياتهم، ما لم يكن ذلك بموافقتهم أو في إطار استثناءات مضبوطة بضمانات[9].

أما على الصعيد الوطني المغربي، فقد استبق المشرع إلى حد ما حماية المعطيات الشخصية بإصدار القانون رقم 08-09 لسنة 2009 (الشهير بـ09-08) المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي[10]. جاء هذا القانون إبان تنامي صناعة مراكز النداء وتدفق البيانات بين أوروبا والمغرب، ليضع قواعد لمعالجة البيانات تهدف إلى حماية خصوصية الأفراد ومواءمة التشريع المغربي مع المعايير الأوروبية. وقد أنشأ القانون هيئة مختصة هي *اللجنة الوطنية لمراقبة حماية المعطيات ذات الطابع الشخصي* (CNDP)لتتولى السهر على إنفاذه. ويتضمن القانون 09-08 مبادئ مشابهة في روحه لتلك الموجودة في التشريعات الأوروبية الأقدم، مثل اشتراط الترخيص أو التصريح المسبق لدى معالجة بيانات شخصية معينة، خاصة إذا كانت حساسة (كالمعطيات حول الأصل العرقي أو الآراء السياسية أو المعتقد الديني أو الحالة الصحية أو البيانات الجينية)، بالإضافة إلى التنصيص على حقوق للأفراد كحق الاعتراض وحق التصحيح. بيد أن مقارنة هذا القانون الوطني بالإطار الأوروبي الحديث تكشف عن وجود فجوات مهمة .فالقانون المغربي – بالرغم من إيجابياته لحظة صدوره – أصبح اليوم متجاوزا في بعض جوانبه ولا يغطي تحديات الذكاء الاصطناعي بما يكفي؛ إذ يفتقر مثلا إلى الإلزام بإشعار الأشخاص في حالة اختراق بياناتهم، ولا يتضمن نصوصا صريحة حول حق محو البيانات أو حق حملها، كما لا يرد فيه ذكر لمبدأ تقليل البيانات ولم يعالج بشكل تفصيلي مسألة رضى الشخص المعني وشروطه في سياق التقنيات الجديدة. كذلك لا توجد في القانون الحالي مقتضيات صريحة حول *تقييم أثر على الخصوصية*

(Privacy Impact Assessment)الواجب إجراؤه قبل إطلاق أنظمة معالجة بيانات شخصية ذات خطورة عالية – وهو إجراء بات ضروريًا في عصر أنظمة الذكاء الاصطناعي ذات القدرات التنبؤية الواسعة.

وعلى المستوى المؤسسي، ورغم الجهود المشهودة التي تبذلها اللجنة الوطنية لحماية المعطيات (CNDP) في المغرب، فإن صلاحياتها الحالية تظل محدودة مقارنة بنظيراتها الأوروبية. فاللجنة تختص بمنح التراخيص ومعالجة الشكايات ويمكنها إحالة المخالفات إلى النيابة العامة، إلا أن سلطاتها الزجرية ليست بالقوة الرادعة الكافية (حيث العقوبات المنصوص عليها في قانون 09-08 تتراوح بين غرامات مالية متواضعة نسبيًا وعقوبات حبسية محدودة في حالات جسيمة). أما في النظام الأوروبي بعد الGDPR، فقد منحت سلطات حماية البيانات صلاحيات واسعة تشمل فرض غرامات ضخمة تصل إلى 4% من رقم معاملات الشركة السنوي العالمي أو 20 مليون يورو (أيهما أعلى) في حال المخالفة الجسيمة. هذا الفارق في مستوى الردع القانوني له أثر ملموس على الامتثال[11]؛ إذ تبدو الشركات العالمية أكثر حرصًا على مراعاة معايير الخصوصية الصارمة في أوروبا، بينما قد لا تولي القدر نفسه من الاهتمام للأسواق التي قوانينها أقل تشددًا. ومن هنا تبرز المخاوف من أن يكون المغرب – وغيره من البلدان ذات الأطر الأضعف – عرضة لاستغلال تقنيات الذكاء الاصطناعي بطريقة تمس خصوصية الأفراد دون الخشية من تبعات قانونية كبيرة.

4. نحو تعزيز الحماية القانونية للخصوصية أمام تحديات الذكاء الاصطناعي

من خلال العرض أعلاه، يتبين أن الحفاظ على الحق في الخصوصية في عصر الذكاء الاصطناعي يستدعي تحديث المنظومة القانونية وتبني جملة من الآليات الوقائية والرقابية. في طليعة هذه الآليات ضرورة إدماج مبدأ" الخصوصية حسب التصميم والافتراضي (Privacy by Design & by Default)" في التشريعات. وهذا المبدأ يفرض على مصممي أنظمة الذكاء الاصطناعي ومطوريها تضمين ضمانات حماية المعطيات الشخصية في صلب تصميم النظام ومنذ المراحل الأولى، وألا يُترك موضوع حماية البيانات كخيار إضافي لاحق. كما ينبغي اشتراط إجراء دراسات أثر على الحياة الخاصة قبل اعتماد أنظمة ذكاء اصطناعي تنطوي على معالجة بيانات حساسة أو اتخاذ قرارات مصيرية بشأن الأفراد، على أن تقدم نتائج هذه الدراسات إلى الهيئة الرقابية (كاللجنة الوطنية) للمصادقة وتقييم مدى كفاية إجراءات الحماية المقترحة.

إضافة لذلك، تبرز أهمية تعزيز شفافية الخوارزميات وحق الأفراد في المعرفة. فإذا كانت أحد أسباب انتهاك الخصوصية هو عدم دراية الشخص بحجم البيانات المجموعة عنه وكيفية استعمالها، فإن القانون يجب أن يكفل حقه في الحصول على معلومات واضحة ومبسطة حول ذلك. وهذا يتطلب إلزام الجهات التي تستخدم أنظمة ذكاء اصطناعي بأن تفصح للمواطنين – بلغة مفهومة – عن نوعية البيانات التي تجمعها وأغراض استخدامها، وعن أي قرارات آلية تتخذ بناءً على تلك البيانات. ومن شأن هذه الشفافية أن تمكن الأفراد من ممارسة حقوقهم (كحق التصحيح أو الحذف) بشكل فعّال وتقديم الشكاوى عند الضرر. كما أن الشفافية التقنية (فتح جزء من تفاصيل عمل الخوارزميات للتدقيق العام عند الحاجة) تساعد الخبراء والجهات المستقلة على تدقيق مدى امتثال الأنظمة لمعايير الخصوصية وعدم انطوائها على تجاوزات.

ولا بد أيضا من تعزيز التعاون الدولي والإقليمي في هذا المجال، نظرًا للطبيعة العابرة للحدود للبيانات وتقنيات الذكاء الاصطناعي. فكما أكدت إحدى الدراسات الحديثة بالمغرب، فإن التعاون الدولي لوضع معايير وقوانين مشتركة بات ضروريا لضمان حماية الحياة الخاصة في عصر التقنية. وهذا ما تسير فيه جهود منظمات كالأمم المتحدة – عبر دعواتها لوضع إطار أممي لمساءلة أنظمة الذكاء الاصطناعي – واليونسكو من خلال توصيتها الأخلاقية عام 2021 التي حثت الدول على تبني مبادئ موحدة لحماية الخصوصية ومشاركة أفضل الممارسات[12]. ومن الجانب العملي، يبقى المغرب بحاجة إلى تسريع ملاءمة تشريعه الداخلي مع المعايير الدولية، لا سيما وأنه طلب منذ 2009 الحصول على قرار الملاءمة مع الاتحاد الأوروبي بخصوص حماية البيانات الشخصية وما زال الطلب قيد الانتظار. وقد خلصت دراسة مقارنة أجرتها السلطات المغربية بشراكة مع الاتحاد الأوروبي إلى سلسلة من الفجوات بين قانون 09-08 وGDPR، ورُسمت ثلاثة سيناريوهات لسد هذه الفجوات:

الإبقاء على القانون دون تعديل، أو تبني الـ GDPR بحذافيره، أو تبني إصلاح "معتدل" يُدخل أهم التعديلات مع مراعاة الخصوصية المحلية. وكان السيناريو الثالث هو الموصى به لتحقيق تقارب تدريجي مع المعايير الأوروبية[13].

وفي المحصلة، فإن حماية الخصوصية أمام تحديات الذكاء الاصطناعي تستوجب تحركا تشريعيا عاجلا يأخذ في الاعتبار: تحديث تعريفات البيانات الشخصية لتشمل الاستدلالات المستنتجة آليا، تقوية سلطات هيئات حماية المعطيات بمنحها موارد وأدوات رقابية أكثر فعالية (بما فيها إجراء عمليات تدقيق منتظمة على أنظمة الذكاء الاصطناعي في المؤسسات العامة والخاصة)، وفرض عقوبات رادعة تتناسب مع جسامة الأضرار المحتملة من خرق الخصوصية في العصر الرقمي. وبدون هذه الخطوات، ستظل حماية الحياة الخاصة للأفراد عرضة للانتقاص مع كل قفزة تقنية جديدة.

ثانيًا: التحديات المرتبطة بالتمييز والتحيز الخوارزمي – نحو مكافحة الآثار التمييزية للذكاء الاصطناعي

1. مخاطر التمييز والتحيز في أنظمة الذكاء الاصطناعي

رغم أن الذكاء الاصطناعي يوصف في كثير من الأحيان بأنه تقنية "محايدة" تستند إلى معادلات رياضية وبيانات موضوعية، فإن الواقع كشف عن جانب مظلم يتمثل في ظاهرة" التحيز الخوارزمي (Algorithmic Bias) "التي يمكن أن تقود إلى قرارات تمييزية وغير عادلة بحق مجموعات معينة من الناس. ينشأ هذا التحيز عادة من عدّة مصادر، أبرزها:

- **تحيّز البيانات المستخدمة لتدريب النظم** :فالخوارزمية تتعلم من البيانات التاريخية المتاحة لها. وإذا كانت تلك البيانات تعكس في طياتها انحيازا اجتماعيا أو عدم مساواة قائما (كعدم تكافؤ الفرص بين جنس وآخر أو مجموعة عرقية وأخرى في مجال ما)، فإن الخوارزمية ستتعلم هذه الأنماط المنحازة وتكرّسها في مخرجاتها المستقبلية. على سبيل المثال، إذا دربنا نظام ذكاء اصطناعي لاختيار الموظفين على بيانات توظيف سابقة في شركة يهيمن عليها الذكور، فقد يستنتج النظام أن المتقدمين الذكور أنسب للوظائف ويقوم بإقصاء المتقدمات الإناث تلقائيا — ليس بناء على الكفاءة الفردية بل استنادا إلى نمط متحيز في البيانات. وهذا ما حدث فعلًا في تجربة معروفة قامت بها إحدى شركات التقنية الكبرى عندما طورت نظاما للتوظيف اتضح أنه يستبعد السير الذاتية التي تحوي لفظ "أنثى" أو إشارات للنساء، لأنه تعلم من بيانات توظيف سابقة منحازة ضد النساء[14].
- **تحيّز خوارزمي ناشئ عن تصميم النموذج** :قد يقوم المصممون (بشكل مقصود أو غير مقصود) بإدخال افتراضات أو معايير في عمل الخوارزمية تؤدي إلى تمييز ضد فئة معينة. مثلا، قرار برمجي بأن تعطي الخوارزمية وزنا أقل لمعايير معينة تتعلق بمجموعة إثنية دون سواها، أو استخدام معايير تبدو ظاهريا محايدة لكنها ترتبط فعليًا بمعايير تمييزية (كأن يستخدم الرمز البريدي كمدخل في تقييم الجدارة الائتمانية، وهو قد يرتبط بمناطق ذات أغلبية عرقية معينة)[15].
- **التحيز في مرحلة تفسير النتائج أو استخدامها** :حتى لو كانت الخوارزمية نفسها عادلة، قد يحدث تمييز في طريقة استعمال نتائجها على أرض الواقع. فعلى سبيل المثال، في أنظمة التصنيف الاجتماعي أو الائتماني، قد تفسر العلامات الممنوحة من الخوارزمية للمرشحين أو المستفيدين بطريقة تمييزية من قبل متخذي القرار من البشر[16].

وتنعكس آثار التحيز الخوارزمي في ميادين عديدة: في التوظيف كما أسلفنا، وفي القطاع المالي حيث رصدت حالات من إعطاء قروض بمعدلات فائدة أعلى أو رفضها بناء على تنبؤات خوارزمية منحازة ضد أقليات، وكذلك في أنظمة العدالة الجنائية حيث برز نقاش عالمي حول عدالة أنظمة التنبؤ الإجرامي) مثل نظام COMPAS في الولايات المتحدة (بعدما تبين أنها قد تظلم المتهمين المنتمين لأعراق معينة عبر تصنيفهم خطِرين بأكثر مما يستحقون[17]. وحتى في الرعاية الصحية وجد أن بعض خوارزميات التصنيف الطبي كانت تمنح أولوية أقل للمرضى

من أصول إفريقية في برامج العناية الصحية بسبب اعتمادها على بيانات إنفاق صحي تاريخية لا تعكس احتياجاتهم الفعلية[18]. هذه الأمثلة تدق ناقوس الخطر بأن الذكاء الاصطناعي، إن لم يوجّه بشكل صحيح، قد يعزز أوجه عدم المساواة القائمة بدل أن يخففها.

المثير للقلق أن التمييز الخوارزمي يكون في الغالب خفيا وغير واضح للمتأثر به. فحين يتعرض شخص ما لقرار سلبي (كرفض وظيفة أو خدمة) ناتج عن نظام ذكاء اصطناعي، قد لا يعرف مطلقا أن التحيز لعب دورا في ذلك، خاصة في ظل الطبيعة "الصندوقية السوداء" لبعض نماذج التعلم العميق التي يصعب تفسير منطقها الداخلي. وهذا يجعل مساءلة هذه الأنظمة أمرا عسيرا، ويطرح تحديا كبيرا أمام تطبيق مبادئ العدالة والمساواة التي تقرها القوانين. إذ كيف يمكن للفرد أن يثبت تعرضه لتمييز غير مشروع إذا كان لا يرى أو يفهم طريقة اتخاذ القرار الآلي؟ بل كيف يمكن للسلطات نفسها اكتشاف ذلك التمييز المستتر؟

2. التأصيل القانوني لمبدأ عدم التمييز في مواجهة المخاطر التقنية

يعتبر مبدأ عدم التمييز والمساواة أمام القانون من الثوابت الراسخة في المنظومات القانونية الحديثة. فالدساتير والتشريعات الوطنية والمواثيق الدولية على حد سواء تحظر التمييز القائم على الجنس أو العرق أو اللون أو الدين أو غيرها من الصفات المحمية. وفي الحالة المغربية، أكد دستور 2011 في ديباجته التزام المملكة بحظر ومكافحة كل أشكال التمييز بسبب الجنس أو اللون أو المعتقد أو الثقافة أو الانتماء الاجتماعي أو الإقليمي أو اللغة أو الإعاقة أو أي وضع شخصي آخر. كما تجرّم القوانين الجنائية والمدنية أي سلوك تمييزي يخل بمبدأ المساواة في التمتع بالحقوق. وعلى الصعيد الدولي، تكفل اتفاقية الأمم المتحدة للقضاء على جميع أشكال التمييز العنصري (ICERD) واتفاقية القضاء على التمييز ضد المرأة (CEDAW) وغيرهما من المعاهدات هذا الحق وتلزم الدول الأطراف باتخاذ تدابير لمنع أي تمييز في ممارسات الدولة أو حتى من قبل الخواص في نطاق الحياة العامة.

بيد أن هذه القواعد القانونية التقليدية وُضعت بالأساس لمعالجة التمييز البشري المباشر (كأن يميز صاحب عمل ضد متقدم بسبب عرقه، أو يرفض مقدم خدمة زبونا بسبب دينه). أما في حالة التمييز الخوارزمي، فإننا إزاء فاعل غير بشري (الخوارزمية) واتخاذ قرار تلقائي قد لا يتضمن نيةً أو قصدا تمييزيا بالمعنى التقليدي، ومع ذلك تُنتج أثرًا يفرق بين الناس على أسس غير موضوعية. هذا يثير تساؤلات مستجدة: هل يمكن اعتبار الخوارزمية بمثابة "طرف" يمارس التمييز لتطبق عليه القواعد؟ ومن يتحمل المسؤولية القانونية عن انحيازه – المصمم أم المستخدم أم الاثنان؟ وكيف نتكيف معايير الإثبات لتأكيد وجود انحياز في نظام تقني معقد؟ هذه الأسئلة تعكس حاجة ملحة لتطوير فهم قانوني جديد لمبدأ عدم التمييز في العصر الرقمي، ووضع آليات خاصة للتعامل معه.

وقد بدأت بعض الأنظمة القانونية والإرشادات التنظيمية تلتفت إلى هذه الإشكالية. فعلى سبيل المثال، تتضمن الـ GDPRالأوروبية نصوصًا حول حق الفرد في عدم الخضوع لقرار آلي محض فيه تمييز، وتعتبر معالجة البيانات "الحساسة" المتعلقة بالعرق أو الدين أو غيرها غير مشروعة إلا بضوابط صارمة، تفاديًا لاستعمالها كمدخلات تمييزية. كما أن مشروع قانون الذكاء الاصطناعي الأوروبي الجديد (EU AI Act) – الذي تم التوافق عليه مؤخرًا في 2024[19] – يجعل من مكافحة التمييز أحد أهدافه الرئيسية. فقد صنّف مشروع القانون أنظمة الذكاء الاصطناعي المستخدمة في مجالات حيوية (كالفرز الوظيفي أو التعليم أو الأمن) ضمن فئة "عالية المخاطر"، وألزم القائمين عليها باتخاذ إجراءات لضمان عدم وجود تحيز أو تمييز في تصميمها وبياناتها، بما في ذلك السماح بمعالجة بيانات حساسة (مثل العرق) لغرض اختبار النظام وكشف ما إذا كان يعطي نتائج منحازة – وهي خطوة لافتة لأنها استثناء لمبدأ منع معالجة البيانات الحساسة، هدفه تمكين المطورين من التعرف على الانحياز وتصحيحه. كذلك أوجبت المسودة على الشركات توفير قدر من الشفافية والتفسير لآلية عمل الأنظمة عالية المخاطر، حتى تتمكن الجهات الرقابية من تقييم مدى عدالتها. ورغم أن هذا القانون (قانون الذكاء الاصطناعي الأوروبي) لم يدخل حيز التنفيذ بعد وقت كتابة هذه الدراسة، إلا أنه يعبر عن توجه تشريعي صاعد لسد الفراغ القانوني فيما يخص التحيز الخوارزمي.

أما في الولايات المتحدة وبعض الولايات تحديدا، فظهرت مبادرات مثل مشروع قانون مساءلة الخوارزميات (Algorithmic Accountability Act)الذي طُرح لأول مرة في 2019 ثم 2022 في الكونغرس الأميركي، ويهدف إلى إلزام الشركات بإجراء تقييمات دورية للانحياز والعدالة في أنظمة الذكاء الاصطناعي التي تؤثر على المستهلكين، وإلى منح هيئات مثل لجنة التجارة الفدرالية صلاحية مراقبة ذلك[20]. وعلى المستوى المحلي، تبنت مدينة نيويورك تشريعا دخل حيز النفاذ عام 2023 يلزم الشركات بإجراء تدقيق مستقل لأنظمة التوظيف الآلية لضمان خلوها من التمييز العرقي أو الجنساني، وإلا تواجه غرامات[21]. هذه الخطوات وغيرها تدل على توجه نحو تقنين الاختبارات الخوارزمية وإدخالها ضمن متطلبات الامتثال القانوني.

في السياق المغربي والعربي عموما، ما زالت مسألة التحيز الخوارزمي جديدة نسبيا على النقاش التشريعي. فلا يوجد نص قانوني صريح حتى الآن يعالج هذه المشكلة، وإن كانت القواعد العامة في تجريم التمييز يمكن نظريًا أن تُطبق على أي قرار أو خدمة — مهما كانت وسيلة اتخاذ القرار — ترتب تمييزا غير مبرر ضد فرد أو مجموعة. بيد أن ذلك يتطلب إقرارا صريحا بأن التمييز الواقع عبر أنظمة تقنية يخضع للمنع ذاته، وربما صدور اجتهادات قضائية تؤكد ذلك. وقد تكون مبادرة وزارة العدل المغربية حاليا لإعداد قانون يؤطّر استخدام الذكاء الاصطناعي فرصة لإدراج مقتضيات تعالج جانبي الشفافية وعدم التمييز في الخوارزميات. كما أن إنشاء وكالة وطنية للذكاء الاصطناعي — وفق ما اقترحه بعض البرلمانيين — من شأنه أن يوفر هيئة يمكنها وضع دلائل توجيهية في هذا المجال ومراقبة مدى مراعاة الأنظمة المستخدمة لمبدأ المساواة.

3. ضمانات قانونية مقترحة لمواجهة التمييز الخوارزمي

يتطلب تفادي الآثار التمييزية للذكاء الاصطناعي اعتماد حزمة من الضمانات القانونية والتقنية تكمل بعضها البعض، ويمكن إيجاز أهمها فيما يلي:

- **الشفافية والتفسير** (**Transparency & Explainability**): كما أسلفنا، لامناص من تعزيز شفافية عمل الخوارزميات بحيث يتسنى كشف أي تحيز في عملياتها. ينبغي أن تفرض القوانين على الجهات المطوِّرة والمستخدِمة للذكاء الاصطناعي توفير قدر ملائم من الشرح حول كيفية اشتغال النظام ومعايير اتخاذه للقرارات، وخاصة في القرارات التي تؤثر على حقوق الأفراد (مثل رفض منح خدمة أو فرصة). إن حق الفرد في *معرفة أسباب القرار المتخذ بحقه* هو حق راسخ في الإجراءات القضائية والإدارية (الحق في تعليل القرارات)، ويجب امتداده إلى القرارات الآلية. فعندما يستطيع الشخص الحصول على شرح لكيفية توصل النظام للنتيجة، سيكون أوعى باحتمال وجود انحياز وبالتالي أقدر على الاعتراض أو طلب المراجعة. وقد أكد خبراء الأمم المتحدة أن انعدام الشفافية يعرقل إمكانية الطعن في القرارات القائمة على الذكاء الاصطناعي وقد يقوض الحق في المحاكمة العادلة وحق التظلم.

- **إخضاع الأنظمة عالية التأثير لتدقيق خوارزمي مستقل** (**Audit**): توجب القواعد المقترحة في أوروبا وبعض الولايات الأمريكية إجراء **اختبارات دورية** لنظم الذكاء الاصطناعي لكشف الانحياز (Bias Audit) من قبل هيئات مستقلة أو خبراء محايدين. ويمكن تقنين ذلك بإلزام المؤسسات الكبيرة التي تعتمد قرارات آلية جماعية بتوفير بيانات وتقارير عن أداء أنظمتها للجهة الناظمة، وإتاحة المجال لإجراء اختبارات تحاكي مخرجات النظام على عينات بيانات مختلفة لاستبيان ما إذا كان يُظهر تحيزا منهجيا ضد فئة ما. هذه العملية شبيهة بالتدقيقات المالية أو تدقيقات الأمن السيبراني، لكنها هنا موجهة للتحقق من **عدالة الخوارزمية**. ولو تبين من التدقيق وجود انحياز غير مبرر، تلزم المؤسسة باتخاذ إجراءات لتعديله (كإعادة تدريب النموذج ببيانات أكثر توازنا، أو تعديل خوارزمية التصنيف) تحت طائلة عقوبات. إن جعل التدقيق الخوارزمي ممارسة معيارية سيسهم في رصد مبكر لأي اختلال قبل أن يتفاقم الضرر، وسيحمل المطورين على تحمل *مسؤولية* مخرجات أنظمتهم والسعي لتحسينها باستمرار.

- **حظر بعض التطبيقات شديدة الخطورة أو تقييدها**: في الحالات التي يُحتمل فيها أن يؤدي استخدام الذكاء الاصطناعي إلى انتهاكات جسيمة لمبدأ المساواة وحقوق الإنسان، قد يكون الخيار الأنسب هو المنع الكلي أو فرض حظر مؤقت لحين وضع ضوابط

ملائمة. وقد دعت مفوضة الأمم المتحدة السامية لحقوق الإنسان إلى **وقف مؤقت لبعض تقنيات الذكاء الاصطناعي** التي تشكل خطرًا بالغًا على حقوق الإنسان إلى أن يتم تطبيق ضمانات كافية. ويأتي ضمن ذلك نظم التصنيف الاجتماعي الشامل (Social Scoring Systems) التي تُقيّم الأشخاص بدرجات يمكن أن تحرمهم من خدمات بناء على سجلهم الرقمي – إذ تحمل مخاطر تمييزية واضحة. كذلك تقنيات التعرف على الوجه في الأماكن العامة تعرض مجموعات معينة (خاصة الأقليات العرقية) لاستهداف غير متناسب نتيجة ارتفاع نسب الخطأ بحقهم، ما دفع دولا ومدنا عدة إلى حظر استخدامها أمنيا إلى أن تثبت نزاهتها. فالقانون يجب أن يتخذ موقفا *احترازيا* حين يتعلق الأمر بتقنيات ظهر جليا أن ضررها على العدالة يفوق منافعها الأمنية أو الاقتصادية.

- **تعزيز حق المراجعة البشرية والتظلم** :ينبغي أن يضمن الإطار القانوني لكل فرد يتأثر سلبا بقرار آلي **حق طلب مراجعة بشرية** لهذا القرار. أي أن لا يكون الحكم النهائي بيد الآلة وحدها دون إمكانية اعتراض. وهذا يتسق مع ما قررته اللائحة GDPR في المادة 22 سالفة الذكر. فتوفر قناة للمراجعة من قبل شخص مؤهل، والنظر في الظروف الخاصة لكل حالة، هو صمام أمان ضد أي أخطاء أو انحياز آلي. وبالتوازي، يجب إرساء إجراءات فعالة لتلقي الشكاوى بخصوص القرارات الآلية وتمكين الأفراد من الطعن أمام جهة قضائية أو إدارية مختصة في مدى مشروعية تلك القرارات. هذه العملية ستضع مسؤولية على عاتق مستخدمي الخوارزميات لتبرير قراراتهم، وتسمح للقضاء بتطوير فقه قانوني في مسائل الذكاء الاصطناعي.

- **المساءلة والمسؤولية القانونية** :(**Accountability**) أخيرًا، لا بد من تحديد واضح للمسؤولية القانونية عندما يؤدي نظام ذكاء اصطناعي إلى قرار تمييزي أو ضرر لفئة معينة. المسؤولية هنا تقع مبدئيا على عاتق **مزود النظام** أو مشغّله الذي استفاد منه واتخذه أداة لاتخاذ القرار. فلا يصح أن يتنصل أحد من تبعات فعل تمييزي بدعوى أن "الخوارزمية فعلت ذلك وليست أنا" – لأن الخوارزمية لا تمتلك شخصية قانونية ولا ذمة مالية؛ ومن ثمّ فمسؤولية نتائجها تقع على من طورها أو استخدمها في عمله. وقد أكد خبراء القانون ضرورة إمكانية نسبة نتائج الأفعال القائمة على الذكاء الاصطناعي إلى شخص ذاتي أو اعتباري يتحمل المسؤولية عند الاقتضاء. وعليه يمكن تحديث القوانين الوطنية (كقانون مكافحة التمييز إن وُجد أو القوانين العامة) بالنص على أن أي *قرار أو إجراء تمييزي* يؤثر في حقوق الأفراد *يحظر مهما تكن وسيلة صنعه*، وأنه في حالة كان هذا القرار آليا فيسأل عنه الشخص الاعتباري أو الذاتي الذي يعتمد على النظام المعلوماتي محل السؤال. ويمكن أيضًا التفكير في استحداث جرائم أو مخالفات إدارية جديدة تعاقب على **الإهمال الجسيم في رقابة الانحياز الخوارزمي**، فمثلا إذا تبين أن جهة ما استخدمت نظاما ذكاء اصطناعيا لمنح قروض وظهر أنه منحاز عرقيًا، تتعرض الجهة للمساءلة والغرامة حتى لو لم يكن هناك قصد تمييزي مباشر، وذلك لردع التساهل مع الانحياز غير المقصود.

بهذه الضمانات المتكاملة، يمكن إيجاد **مقاربة استباقية** تحد من مخاطر التمييز والتفاوت الاجتماعي الذي قد ينتج عن استخدام واسع وغير مضبوط للذكاء الاصطناعي. ويبقى التحدي في القدرة على إنفاذ هذه الضوابط عمليا ومواكبتها للتطور السريع في التقنيات، وهو ما يتطلب بدوره تعزيز الخبرات التقنية لدى الجهات القضائية والمؤسسات الوطنية المعنية بحقوق الإنسان.

- **خاتمة واستنتاجات وتوصيات**

خلصت هذه الدراسة إلى أن تنامي الاعتماد على تقنيات الذكاء الاصطناعي في مختلف مناحي الحياة يفرض تحديات غير مسبوقة على منظومة الحقوق والحريات، وفي مقدمتها الحق في الخصوصية ومبدأ عدم التمييز. وقد تبين أن الإطار القانوني التقليدي – سواء على المستوى الدولي أو في التشريع الوطني المغربي – يحتاج إلى تحديث عميق لسد الثغرات التي كشفتها الثورة الرقمية. فالخصوصية الرقمية باتت مهددة بأساليب مستترة لجمع البيانات الشخصية واستغلالها على نطاق واسع، ما لم توجد قواعد صارمة لضبط الأمر وضمان سيادة إرادة الأفراد على معطياتهم .كذلك أضحى التمييز الخوارزمي خطرا حقيقيا يمكن أن يقوّض عقودًا من الجهود التشريعية لمكافحة التمييز القائم على الجنس أو العرق أو غيرهما، إذ يمكن للخوارزميات – دون رادع أو رقابة – أن تعيد إنتاج أنماط الإقصاء بشكل آلي يصعب رصده.

وعلى ضوء المقارنة بين النموذج الأوروبي المتقدم والحالة المغربية، يتضح أن المغرب قطع شوطا معتبرا بإقراره قانون حماية المعطيات الشخصية عام 2009 وتأصيل الحق في الخصوصية دستوريا، إلا أن تطورات العقد الأخير تجعل ذلك غير كاف. فثمة حاجة ملحة لإصلاح تشريعي شامل: يتمثل أولاً في تحديث قانون 09-08 ليتلاءم مع مبادئ ومعايير الGDPR، من حيث توسيع حقوق الأفراد (بإضافة حق النسيان ونقل البيانات مثلا) وتعزيز متطلبات الأمان والإخطار عن الخروقات وإدخال مفهوم تقييم أثر المعالجة عالية المخاطر وإلزامية تعيين مسؤولي حماية البيانات في المؤسسات الكبرى، إضافة إلى رفع سقف العقوبات على المخالفين لجعلها ذات أثر رادع. وثانيًا، إصدار قانون خاص بتنظيم الذكاء الاصطناعي يُحدد مجالات استخدامه وضوابط ذلك الاستخدام ضمن إطار أخلاقي وقانوني يحظر ما قد يسيء إلى الحقوق الأساسية. وينبغي أن يتضمن هذا القانون نصوصًا صريحة حول منع التمييز الآلي ووجوب شفافية القرارات الخوارزمية، على غرار ما تتجه إليه التشريعات الأوروبية الحديثة. كما يمكن أن ينشئ هيئات أو لجان متخصصة تُعنى بوضع سياسات وطنية في هذا الصدد وتنسيق جهود مختلف الفاعلين.

علاوة على الإصلاح القانوني، أوصت الدراسة بعدة تدابير مكملة، من بينها :تعزيز قدرات هيئة حماية المعطيات الشخصية (CNDP) بشريا وتقنيا كي تضطلع بدور رقابي أكثر فعالية، بما في ذلك مراقبة استخدامات الذكاء الاصطناعي في القطاعين العام والخاص وإصدار دلائل إرشادية ملزمة حولها. وكذلك إدماج أخلاقيات الذكاء الاصطناعي ضمن مناهج تكوين المهندسين ورجال القانون على حد سواء، لضمان فهم متبادل للتحديات وتقارب في إيجاد الحلول. كما شددت الدراسة على أهمية التوعية المجتمعية بخطورة القبول الأعمى بمخرجات الخوارزميات، وضرورة مطالبة الأفراد والشركات معًا بالشفافية واحترام الخصوصية – فالمجتمع الواعي يشكل خط الدفاع الأول عن حقوقه.

وعلى الصعيد الدولي، يستحسن انخراط المغرب بفاعلية في المبادرات الأممية والإقليمية ذات الصلة، سواء عبر المصادقة على اتفاقية مجلس أوروبا رقم 108 المعدلة (لحماية الأفراد تجاه المعالجة الآلية للمعطيات ذات الطابع الشخصي) والتي فتحت للدول غير الأعضاء، أو عبر دعم تنفيذ توصية اليونسكو لأخلاقيات الذكاء الاصطناعي (2021) على المستوى الوطني. فمثل هذه الخطوات تعزز موقع المغرب كبلد ملتزم بحماية الحقوق في البيئة الرقمية، وتيسر نقل المعرفة والخبرة في هذا الميدان سريع التطور.

وختامًا، تؤكد الدراسة أن الذكاء الاصطناعي سلاح ذو حدين :فهو من جهة فرصة ذهبية لتحقيق التنمية المستدامة وتحديث الاقتصاد وتحسين الخدمات، ومن جهة أخرى قد يصبح أداة للإخلال بالخصوصيات وتكريس التمييز إذا ترك دون كوابح قانونية وأخلاقية. وعليه فإن المسؤولية تقع على كاهل المشرع وصانع القرار اليوم أكثر من أي وقت مضى ليضعوا الأطر والضمانات التي تكفل أن تبقى هذه التقنيات خادمة للإنسان وقيمه، لا منتهكة لحقوقه وحرياته. وإن بناء الثقة في منظومة الذكاء الاصطناعي يستلزم حوكمة رشيدة لهذه التقنيات ترتكز على الشفافية والمساءلة واحترام الكرامة الإنسانية. بذلك فقط يمكن للمجتمع أن يجني ثمار الذكاء الاصطناعي بأمان، مطمئنا إلى أن القانون يحميه من مخاطره، وأن حقوقه المصونة دستوريا ستظل محمية في كل زمان ومكان، حتى وفي قلب الثورة الرقمية.

الهوامش:

[1] -European Union. General Data Protection Regulation (GDPR). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016. Official Journal of the European Union, L119, 4 May 2016, pp. 1–88.

[2]– مجلس النواب المغربي. (2024، 19 مارس). مقترح قانون بشأن تنظيم استعمال الذكاء الاصطناعي، مقترح للفريق الحركي. الرباط: مجلس النواب. متاح على الموقع الرسمي لمجلس النواب: https://2u.pw/nlmDY (تاريخ الاطلاع: 15 يونيو 2025).

[3] - Office of the United Nations High Commissioner for Human Rights (OHCHR), The Right to Privacy in the Digital Age, 2014. https://www.ohchr.org/en/issues/digitalage/pages/digitalageindex.aspx

[4]– دستور المملكة المغربية لسنة 2011، الجريدة الرسمية عدد 5964 مكرر، الصادرة بتاريخ 30 يوليوز 2011، الفصل 24.

[5]– منظمة الأمم المتحدة للتربية والعلم والثقافة (اليونسكو)، توصية بشأن أخلاقيات الذكاء الاصطناعي، الدورة 41 للمؤتمر العام، القرار رقم 37، باريس، 23 نوفمبر 2021، ص. 8. https://unesdoc.unesco.org/ark:/48223/pf0000381137

[6]– مفوضية الأمم المتحدة السامية لحقوق الإنسان، *الحق في الخصوصية في العصر الرقمي*، تقرير المفوض السامي المقدم إلى الجمعية العامة، الوثيقة رقم : A/HRC/39/29، 3 أغسطس 2018، الفقرات 10–13. https://undocs.org/A/HRC/39/29

[7]- United Kingdom, House of Commons Digital, Culture, Media and Sport Committee, Disinformation and 'fake news': Final Report, Eighth Report of Session 2017–19, published 14 February 2019, HC 1791, pp. 6–10.

[8] - OECD, Artificial Intelligence in Society, OECD Publishing, Paris, 2019, p. 146. https://doi.org/10.1787/eedfee77-en

[9]– الاتحاد الأوروبي، اللائحة العامة لحماية البيانات (GDPR)، التنظيم رقم 679/2016 الصادر عن البرلمان الأوروبي والمجلس بتاريخ 27 أبريل 2016، الجريدة الرسمية للاتحاد الأوروبي، L119، 4 ماي 2016، المواد 5، 6، 7، 12–23، و34. https://eur-lex.europa.eu/eli/reg/2016/679/oj

[10]– المملكة المغربية، القانون رقم 09.08 المتعلق بحماية الأشخاص الذاتيين تجاه معالجة المعطيات ذات الطابع الشخصي، الصادر بتنفيذه الظهير الشريف رقم 1.09.15 بتاريخ 18 فبراير 2009. https://2u.pw/a4asq

[11]– الاتحاد الأوروبي، اللائحة العامة لحماية البيانات (GDPR)، التنظيم رقم 679/2016، المادة 83

[12]– اليونسكو، توصية بشأن أخلاقيات الذكاء الاصطناعي، القرار 41 C/37، باريس، 2021، ص. 9–12. https://unesdoc.unesco.org/ark:/48223/pf0000381137

[13]– اللجنة الوطنية لمراقبة حماية المعطيات الشخصية (CNDP)، بيان صحفي: التقارب بين القانون المغربي 09-08 واللائحة الأوروبية العامة لحماية البيانات RGPD، الرباط، 7 يوليوز 2018. https://www.cndp.ma/convergence-entre-la-loi-marocaine-09-08-et-le-nouveau-reglement-europeen-sur-la-protection-des-donnees-personnelles-rgpd

[14] - Dastin, Jeffrey. Amazon scrapped 'sexist AI' recruiting tool, Reuters, 10 October 2018. https://www.reuters.com/article/us-amazon-com-jobs-automation-insight-idUSKCN1MK08G

[15] - Barocas, Solon; Hardt, Moritz; and Narayanan, Arvind. Fairness and Machine Learning: Limitations and Opportunities, fairmlbook.org, 2019, Chapter 5: "Sources of Bias", pp. 87–98. https://fairmlbook.org/

[16] - Mittelstadt, Brent D. Principles alone cannot guarantee ethical AI, Nature Machine Intelligence, Vol. 1, 2019, pp. 501–507. https://www.nature.com/articles/s42256-019-0114-4

[17] - Angwin, Julia et al., Machine Bias: There's software used across the country to predict future criminals. And it's biased against blacks, ProPublica, May 23, 2016. https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

[18] - Obermeyer, Ziad et al., Dissecting racial bias in an algorithm used to manage the health of populations, Science, Vol. 366, Issue 6464, October 2019, pp. 447–453. https://www.science.org/doi/10.1126/science.aax2342

[19] - المفوضية الأوروبية، مشروع قانون الذكاء الاصطناعي (AI Act): مقترح لائحة بشأن القواعد المنسقة على مستوى الاتحاد الأوروبي في مجال الذكاء الاصطناعي، الوثيقة المرجعيةCOM(2021) 206 final :، بروكسيل، آخر تحديث: التوافق السياسي النهائي في مارس 2024 .النص الكامل متاح عبر: https://artificialintelligenceact.eu

[20] - U.S. Congress, Algorithmic Accountability Act of 2022, Bill S.3572 – Introduced in the Senate on February 2, 2022. https://www.congress.gov/bill/117th-congress/senate-bill/3572

[21] - NYC Council, Local Law No. 144 of 2021, "Automated Employment Decision Tools" Law, effective January 1, 2023.