ISSN(Print): 1813-4521 OnLine ISSN:2663-7502
Journal Of the Iraqia University
available online at: https://www.mabdaa.edu.iq

مكانة الذكاء الاصطناعي في السياسة الجنائية الوقائية؛ دراسة مقارنة في قوانين العراق وإيران والإمارات العربية المتحدة

الدكتور قماشي، عضو الهيئة العلمية في كلية القانون
أحمد راضي عزيز، طالب دكتوراه في القانون
جامعة كاشان / كلية القانون

The Position of Artificial Intelligence in Preventive Criminal Policy: A Comparative Study of the Laws of Iraq, Iran, and the United Arab Emirates

Researcher: AHMAD RADI AZIZ
Responsible author: Dr. Saeed Ghomashi
University of Kashan / Faculty of Law
Responsible author: Saeed Ghomashi@yahoo.com

Abstract

This study examines the position of artificial intelligence in preventive criminal policy and evaluates its legal capacities in the legal systems of Iraq, Iran, and the United Arab Emirates. The main issue is how to reconcile the use of data- and algorithm-based systems in the stages preceding crime control, the identification of high-risk situations, and the direction of preventive interventions with the requirements of the rule of law, human dignity, privacy, and fair trial. The research follows an analytical-comparative method based on higher legal documents, substantive and procedural criminal laws, rules of electronic evidence, data-protection rules, and related practices. The findings show that the three systems have provided normative grounds for accepting electronic data and documents, expanding jurisdiction over cybercrimes, and relying on digital evidence. However, the absence of specific rules on algorithmic transparency, effective human oversight, high-risk processing impact assessment, responsibility for systemic error, and safeguards against automated discrimination remains a shared gap.**Keywords:** artificial intelligence, crime prediction, crime prevention, criminal policy, personal data, electronic evidence, Iran, Iraq, United Arab Emirates.

المستخلص

أُنجز هذا البحث بهدف بيان مكانة الذكاء الاصطناعي في السياسة الجنائية الوقائية وتقويم طاقاته القانونية في ثلاثة أنظمة قانونية، هي إيران والعراق والإمارات العربية المتحدة. وتتمثل المسألة الرئيسة في كيفية التوفيق بين الاستفادة من النظم القائمة على البيانات والخوارزميات في المراحل السابقة على السيطرة على الجريمة، وتحديد الأوضاع عالية الخطورة، وتوجيه التدخلات الوقائية، وبين مقتضيات سيادة القانون والكرامة الإنسانية والخصوصية والمحاكمة العادلة. وتعتمد منهجية البحث على المنهج التحليلي المقارن، بالاستناد إلى دراسة الوثائق العليا، والقوانين الجنائية الموضوعية والإجرائية، وقواعد الأدلة الإلكترونية، وقواعد حماية البيانات، والممارسات ذات الصلة. وتبين النتائج أن الأنظمة الثلاثة وفرت الأسس المعيارية اللازمة لقبول البيانات والمستندات الإلكترونية، وتوسيع الاختصاص في الجرائم المعلوماتية، والاستفادة من الأدلة الرقمية، بما يتيح استخدام مخرجات نظم الذكاء الاصطناعي في التقييم القضائي والتدابير الوقائية. غير أن غياب قواعد خاصة تتعلق بالشفافية الخوارزمية، والرقابة الإنسانية الفعالة، وتقييم أثر المعالجة عالية الخطورة، والتحديد الدقيق للمسؤولية عن الخطأ النظامي، والضمانات الكافية ضد التمييز الآلي، يمثل فراغا ،مشتركا بين هذه الأنظمة. وتكشف المقارنة بين الدول الثلاث أن الإمارات، من خلال سن قوانين منسقة في مجال حماية البيانات الشخصية والمعاملات الإلكترونية، والعدالة الجنائية الإلكترونية، تمتلك إطارا أكثر تقدما لإدماج الذكاء الاصطناعي في السياسة الجنائية الوقائية. أما إيران فقد أنشأت طاقات مهمة في مجال الجرائم المعلوماتية، والأدلة الإلكترونية، ومسؤولية الأشخاص المعنوية، لكنها تفتقر إلى قانون عام لحماية البيانات وإلى قواعد صريحة بشأن اتخاذ القرار الآلي. أما العراق، فبالاستناد إلى مرونة قواعد الإثبات وتأكيد الدستور حرية الاتصالات والكرامة

الإنسانية، يملك أرضية معيارية ملائمة لقبول الأدلة الرقمية وتقييد الرقابة الخوارزمية، وإن كان يواجه نقائص جدية على مستوى التنفيذ المؤسسي والتنظيم الفني.

الكلمات المفتاحية: الذكاء الاصطناعي، التنبؤ بالجريمة، الوقاية من الجريمة، السياسة الجنائية، البيانات الشخصية، الأدلة الإلكترونية، إيران، العراق، الإمارات العربية المتحدة.

بيان المسألة

حيث تتطور التقنيات الحديثة والمتقدمة بسرعة كبيرة، يعد مجال مكافحة الجريمة من أكثر المجالات تأثرا بتقدم الذكاء الاصطناعي، ولا سيما في المجالات القضائية والأمنية. فالذكاء الاصطناعي، بوصفه أداة قوية في التنبؤ بالجرائم والوقاية منها ومكافحتها، أخذ ينفذ بسرعة إلى الأنظمة القضائية في مختلف الدول. وتمتلك هذه التقنية، بما لها من قدرات على تحليل البيانات ومحاكاة السلوك الإجرامي والتنبؤ بوقوع الجرائم، قابلية تغيير البنى التقليدية للأنظمة القضائية والأمنية. ومع ذلك فإن هذا التقدم يثير تحديات ملحوظة في المجال القانوني، ولا سيما في دول إيران والعراق والإمارات العربية المتحدة. ويعنى هذا النص ببحث الطاقات القانونية لاستخدام الذكاء الاصطناعي في التنبؤ بالجرائم والوقاية منها في هذه الدول الثلاث، وبتحليل التحديات القانونية القائمة في هذا المجال.تتمثل إحدى المسائل الرئيسة التي تبرز عند استخدام الذكاء الاصطناعي في مكافحة الجرائم في ضرورة مراعاة المبادئ والطاقات القانونية عند استعمال هذه التقنية. ففي دول مختلفة، ولا سيما في إيران والعراق، لم يدخل الذكاء الاصطناعي بعد، في جوانب كثيرة، ضمن إطار قوانين جزائية دقيقة وواضحة. وقد يؤدي ذلك إلى مخاطر من قبيل انتهاك خصوصية الأفراد ووقوع مظالم في الإجراءات القضائية. ومن ثم فإن أحد الأسئلة الأساسية هو كيفية توظيف الذكاء الاصطناعي ضمن إطار القوانين الجزائية في الدول المذكورة، من غير أن تتعرض حقوق الإنسان وخصوصية الأفراد للخطر .يعد الحفاظ على خصوصية الأفراد أحد التحديات الرئيسة. فاستخدام الذكاء الاصطناعي في تحليل البيانات المرتبطة بالجريمة، مثل المعلومات المتعلقة بكاميرات المراقبة، وتتبع الأشخاص، وتحليل البيانات السيبرانية، يقتضي الوصول إلى حجم كبير من المعلومات الشخصية. وفي إيران، ومن أجل مواجهة هذه التحديات، تناول قانون الجرائم المعلوماتية حماية البيانات الفردية بجدية، وعد الاستعمال غير المصرح به لهذه البيانات مخالفة قانونية. وتحظر هذه القواعد بوضوح استخدام البيانات الشخصية من دون إذن، وتوجب المعالجة القانونية لانتهاك الخصوصية. وفي الإمارات كذلك توجد قواعد مماثلة تؤكد أن استخدام البيانات الشخصية يجب أن يتم وفقا لقوانين حماية الخصوصية.يمثل غياب القوانين الشاملة والمحددة لاستخدام الذكاء الاصطناعي في النظام القانوني تحديا آخر في هذا المجال. فعلى الرغم من أن بعض القوانين في إيران والإمارات، مثل قانون الجرائم المعلوماتية وقانون الإجراءات الجزائية، أشارت بصورة غير مباشرة إلى موضوعات تتصل بالتقنيات الحديثة، فإن أيا من هذه الدول لم يسن بعد قانونا شاملا ومحددا بشأن استخدام الذكاء الاصطناعي في النظام القضائي. ويؤدي هذا الفراغ القانوني إلى مواجهة استخدام هذه التقنيات في الإجراءات القضائية لإبهامات وتحديات متعددة. ففي إيران، على سبيل المثال، لم تتناول القوانين القائمة بصورة كاملة وشاملة مسائل مثل المسؤولية عن استخدام الذكاء الاصطناعي، وكيفية جمع البيانات، وطريقة استعمالها، وهو ما يفضي إلى غياب الشفافية في المسارات القضائية. وفي الإمارات أيضا، وعلى الرغم من الجهود المتواصلة لصياغة قوانين حديثة، ما تزال القوانين الخاصة باستخدام الذكاء الاصطناعي في مجال القانون الجزائي غير قائمة بصورة كافية.تبدو الحاجة إلى سن قوانين جديدة وشاملة لاستخدام الذكاء الاصطناعي في الإجراءات القضائية حاجة ملحة. ففي إيران على وجه الخصوص، ونظرا إلى التعقيدات القانونية القائمة، تبرز ضرورة سن قانون خاص لاستخدام الذكاء الاصطناعي وتحديد الحقوق والمسؤوليات في هذا المجال بدقة. وكذلك في الإمارات، ومع الاتساع المتزايد في استخدام هذه التقنية، يصبح سن قوانين جديدة واستكمال القوانين الحالية ضروريا لتغطية استخدام الذكاء الاصطناعي على المستويين الوطني والدولي بصورة أفضل.

المبحث الأول: الأطر القانونية والوثائق العليا الناظمة للوقاية التقنية

إن تحليل الطاقات القانونية للتنبؤ بالجريمة والوقاية منها على أساس الذكاء الاصطناعي في النظام القانوني الإيراني، على مستوى الوثائق العليا والأطر التشريعية العامة، يقتضي بالضرورة الالتفات إلى مكانة الأشخاص المعنوية في بنية الاستجابة الجنائية، لأن جزءا كبيرا من تصميم النظم الذكية ونشرها واستثمارها يقع بيد مؤسسات عامة وخاصة، ومن دون تنظيم دقيق لمسؤوليتها والجزاءات المقررة بحقها تبقى كل سياسة وقائية تقنية في حدود توصية نظرية. وفي الوقت نفسه، فإن القانون الجنائي الإيراني، إلى جانب العقوبات الثابتة في الحدود والقصاص والديات، يجعل نطاق التعزيرات المجال الرئيس لممارسة سلطة القاضي في تحديد نوع العقوبة ومقدارها، وهذا المنطق القائم على سلطة قضائية مقيدة في التعزيرات يوفر أرضية لتنظيم الاستجابة الجنائية إزاء السلوكيات التقنية عالية الخطورة. وقد قرر قانون العقوبات الإسلامي لسنة ١٣٩٢ في المادة ٢٠، بالإحالة

إلى المادة ١٤٣، نظاما خاصا للمسؤولية الجنائية للأشخاص المعنوية، فنص على أنه متى عُد الشخص المعنوي مسؤولا على أساس المادة ١٤٣، فإنه يحكم عليه، بحسب جسامة الجريمة ونتائجها الضارة، بواحدة أو اثنتين من العقوبات المقررة، مثل الحل، ومصادرة جميع الأموال، والمنع من نشاط مهني أو اجتماعي واحد أو أكثر، والمنع من الدعوة العامة لزيادة رأس المال، والمنع من إصدار بعض السندات التجارية، والغرامة، ونشر حكم الإدانة في وسائل الإعلام. كما تحدد المادة ٢١ من القانون نفسه مقدار الغرامة التي يجوز فرضها على الأشخاص المعنوية بما لا يقل عن ضعف المبلغ المقرر للأشخاص الطبيعيين ولا يزيد على أربعة أضعافه. وترسم هاتان المادتان معا الإطار العام للمسؤولية والجزاءات الحاكمة للأشخاص المعنوية المستفيدة من نظم الذكاء الاصطناعي في سياسة الوقاية، وتدلان على أن المشرع توقع مسبقا إمكان التدخل الجنائي في مواجهة سوء الاستغلال أو الإهمال المؤسسي في تطبيق التقنيات الذكية.[١]تدل العقوبات المنصوص عليها في المادة ٢٠ من قانون العقوبات الإسلامي لسنة ١٣٩٢، ولا سيما إمكان حل الشخص المعنوي، ومصادرة جميع أمواله، ومنعه من ممارسة نشاط مهني أو اجتماعي، ونشر الحكم في وسائل الإعلام، على أن المشرع أراد إخراج المسؤولية الجنائية للأشخاص المعنوية من المستوى الرمزي وتحويلها إلى أداة فعالة لتنظيم السلوك. وفي مجال الوقاية التقنية من الجريمة، يعني ذلك أن المصارف، وشركات الاتصالات، والمنصات الافتراضية الكبرى، والشركات المقدمة لخدمات تحليل البيانات، بل وحتى بعض المؤسسات العامة التي تدخل النشاط الاقتصادي في صورة شخص معنوي، ستواجه طيفا واسعا من الردود الجنائية إذا استثمرت نظم الذكاء الاصطناعي على نحو يؤدي إلى ارتكاب جرائم معلوماتية، أو انتهاك أسرار المواطنين وخصوصية بياناتهم، أو تسهيل وقوع جرائم منظمة. وهذا الاحتمال نفسه يعمل، من منظور السياسة الجنائية، حافزا قويا لإنشاء آليات رقابة داخلية، وصياغة تعليمات أخلاقية وقانونية في تطوير الخوارزميات، وإنشاء وحدات للامتثال القانوني، وتصميم نظم لتسجيل أداء النظم الذكية ورصده، وبذلك تتحول الطاقة القانونية للنص إلى عامل وقائي.[٢]تعد المادة ٢١ من قانون العقوبات الإسلامي لسنة ١٣٩٢، التي تقرر أن مقدار الغرامة المفروضة على الأشخاص المعنوية لا يقل عن ضعف الغرامة المقررة للأشخاص الطبيعيين ولا يزيد على أربعة أضعافها، مكملا مهما للمادة ٢٠ في إطار الطاقات القانونية للوقاية التقنية. فزيادة نطاق الغرامة بما يتناسب مع الوضع المالي للأشخاص المعنوية لا تحقق عدالة نسبية في تحمل عبء العقوبة فحسب، بل تؤدي أيضا دورا رادعا خاصا في مواجهة شركات التقنية الكبرى، والمصارف، والمؤسسات المالية والائتمانية التي قد تميل، سعيا إلى زيادة الربح، إلى استخدام نظم الذكاء الاصطناعي في تحليل البيانات والقرارات الائتمانية على نحو يخلط بين التقييم المشروع للخطر وبين التمييز أو انتهاك الخصوصية. وعندما يقرر المشرع صراحة أن غرامة الأشخاص المعنوية تكون مضاعفة قياسا إلى الأشخاص الطبيعيين، فإنه يذكر هذه الكيانات بأن كلفة تجاهل المتطلبات القانونية في استعمال الذكاء الاصطناعي وسائر التقنيات المتقدمة قد تكون باهظة جدا، بل قد تتجاوز أحيانا المنافع القصيرة الأجل الناتجة عن الاستغلال غير المسؤول.[٣]

المطلب الأول: مكانة الوقاية من الجريمة في الدستور والقوانين الجنائية الإيرانية

في السياسة الجنائية للجمهورية الإسلامية الإيرانية، تتشكل مكانة الوقاية من الجريمة في ارتباط وثيق بأسس الدستور والقوانين الجنائية العادية، ويعد قانون الجرائم المعلوماتية الصادر في ١٣٨٨/٠٣/٠٥، ولا سيما مادته ٢٧، نموذجا واضحا لترجمة هذه الأسس إلى تدابير محددة في مجال الجرائم المستحدثة. فالقاعدة العامة في الدستور أن السلطة القضائية، إلى جانب الفصل في الدعاوى وإصدار الأحكام ومعاقبة المجرمين، تضطلع كذلك بمهمة اتخاذ التدابير اللازمة للوقاية من وقوع الجريمة، وبذلك لا تكون الوقاية أمرا هامشيا، بل وظيفة بنيوية في نظام العدالة الجنائية. وقد تجلى هذا الاتجاه في القوانين الجنائية العادية من خلال توقع مؤسسات مثل تعليق التعقيب، وتعليق تنفيذ العقوبة، والعقوبات التكميلية، والتدابير الأمنية والتربوية. وفي مجال الجرائم المرتبطة بتقنية المعلومات، سعى المشرع، عبر تقرير عقوبات خاصة تقيد الوصول إلى البنى الرقمية، ومع مراعاة أن بنى مثل الاتصالات الشبكية ونظم التعرف وتحليل البيانات يمكن أن تكون في الوقت نفسه بيئة لارتكاب الجريمة وأداة للرقابة والتدخل المبكر، إلى إيجاد تداخل بين الرد الجنائي والسيطرة الموجهة على الخطر. وفي هذا الإطار، تكشف المادة ٢٧ من قانون الجرائم المعلوماتية، بتأكيدها إمكان حرمان الفرد من الخدمات الإلكترونية العامة في حالة تكرار الجريمة المعلوماتية، عن مكانة الوقاية من الجريمة في قلب السياسة الجنائية التقنية، وتبين أن المشرع لم يعد الوصول غير المقيد إلى الأدوات التقنية أمرا محايدا، بل نظر إليه بوصفه مصدرا محتملا للخطر ينبغي ضبطه في مواجهة سوء الاستعمال. وتنص هذه المادة على أنه في حالة تكرار الجريمة المعلوماتية أكثر من مرتين، يجوز للمحكمة، بحسب نوع الجريمة وجسامتها وعقوبتها الأصلية، أن تحرم المرتكب مدة من شهر إلى خمس سنوات من الخدمات الإلكترونية العامة مثل الاشتراك في الإنترنت، والهاتف المحمول، والحصول على النطاق الوطني الأعلى، والخدمات المصرفية الإلكترونية، وبذلك تنشأ صلة وقائية بين العقوبة التقليدية والحرمان التقني.[٤]يقوم المنطق الداخلي للمادة ٢٧ من قانون الجرائم المعلوماتية على الربط بين تكرار الجريمة، وخطورة الشخص، وضبط الوصول إلى أداة الارتكاب، بحيث يفترض

المشرع في الجرائم المعلوماتية أن أداة الارتكاب وبيئة وقوع الجريمة هما البنية ذاتها للخدمات الإلكترونية العامة، وأن خطر تكرار السلوك الإجرامي يظل قائما ما دام المرتكب يملك وصولا كاملا وغير مقيد إلى هذه البنى. ومن هذا المنظور، لا تعني الوقاية من الجريمة في هذا القانون مجرد توصية أخلاقية أو برنامج اجتماعي، بل تصاغ في قاعدة ملزمة تتيح للمحكمة، بعد ثبوت التكرار، قطع أو تقييد حلقة اتصال الفرد بالبيئة المنتجة للجريمة لمدة محددة وموجهة. وينسجم هذا النظر مع الأسس العامة للوقاية في القانون الجنائي الإيراني، لأن الفلسفة الرئيسة في مؤسسات مثل العقوبات التكميلية والتدابير الأمنية تقوم كذلك على إزالة أو إضعاف الظروف التي تسهل ارتكاب الجريمة، من غير أن تستند بالضرورة إلى تشديد الألم البدني أو المالي. فالحرمان من الإنترنت عالي السرعة، أو تعطيل إمكان تسجيل النطاق الوطني الأعلى، أو تقييد الخدمات المصرفية الإلكترونية بالنسبة إلى شخص استخدم هذه البنى مرارا في الاحتيال المعلوماتي أو الوصول غير المشروع إلى البيانات أو نشر المحتوى الإجرامي، يمثل في الواقع نموذجا للوقاية الخاصة المصممة بما يتناسب مع طبيعة الجريمة وطريقة ارتكابها، إذ تخفض احتمال التكرار من خلال تقليل الفرصة وتعقيد إعادة استخدام أداة الجريمة.[٥] يتضح ارتباط المادة ٢٧ من قانون الجرائم المعلوماتية بسياسة الوقاية من الجريمة في الدستور وسائر القوانين الجنائية عندما توضع إلى جانب دور السلطة القضائية في اتخاذ التدابير الوقائية، وإلى جانب المؤسسات الخاصة بالوقاية في القوانين العادية. فالسلطة القضائية، وفقا لمبادئ الدستور، ملزمة بالتخطيط لتقليل أسباب وقوع الجريمة، وقد جرى تنفيذ هذه المهمة في السنوات الأخيرة من خلال إنشاء مجالس ومعاونيات متخصصة في الوقاية وصياغة لوائح في مجال الجرائم السيبرانية والأدلة الإلكترونية. وفي هذا المناخ، ينظر إلى الحرمان التقني المنصوص عليه في المادة ٢٧ بوصفه أداة قانونية بيد القاضي للسيطرة على الخطر، يمكن أن تساعد، بالتنسيق مع تدابير أخرى مثل تعليم المستخدمين، ورفع أمن النظم، والرقابة على نشاط مقدمي الخدمات، في خفض الجرائم المعلوماتية، بشرط أن تنظم معايير فرض هذا الحرمان بصورة شفافة وقابلة للتفسير، حتى تكون صلته بأدلة القضية وأهداف الوقاية قابلة للتتبع بوضوح، وحتى تقل إمكانية التحيز أو التعسف في القرار. ومن جهة أخرى، فإن قانون العقوبات الإسلامي، بتوقعه عقوبات تكميلية مثل المنع من مزاولة بعض المهن، أو المنع من الإقامة في بعض المناطق، أو الإلزام بالإقامة في مكان معين، يبين أن السياسة الجنائية الإيرانية تسعى إلى الوقاية من الجريمة عبر تقييد الفرص المنتجة للجريمة، ويمكن عد المادة ٢٧ من قانون الجرائم المعلوماتية امتدادا لهذا المنطق في الفضاء الافتراضي، مع فارق أن الأمر هنا لا يتعلق بمنع الحركة في البيئة المادية، بل بمنع الحضور في البنى الرقمية.[٦] إن استخدام الحرمان التقني بوصفه أداة للوقاية الخاصة يمكن أن يصبح هو نفسه مصدرا لتحديات من زاوية حقوق المواطنة والوظائف المشروعة للتقنية، وهذا ما يجعل مكانة هذا التدبير بين السياسات الوقائية شديدة الحساسية. فالوصول إلى الإنترنت والهاتف المحمول والخدمات المصرفية الإلكترونية يؤدي في الحياة الاجتماعية الراهنة دورا يتجاوز الخدمة الرفاهية المحضة، ويرتبط عمليا بحقوق مثل الوصول إلى المعلومات، وحق المشاركة الاقتصادية والاجتماعية، بل وإمكان الانتفاع ببعض الخدمات العامة. وفي الوقت نفسه، أدى هذا الوصول السهل والواسع إلى الأدوات الذكية إلى خفض عتبة ارتكاب بعض السلوكيات الإجرامية بصورة ملحوظة، وإلى إبراز التعارض بين الحاجة إلى حماية المجتمع وضرورة صون قنوات الانتفاع المشروع بالتقنية. ومن ثم فإن الحرمان الطويل الأمد من هذه الخدمات، على الرغم من أنه يبدو ظاهريا عقوبة قليلة الخطر، قد يفضي إلى عزلة الفرد، وإضعاف إمكان إعادة إدماجه اجتماعيا، بل ودفعه إلى وسائل غير قانونية لتجاوز القيود. لذلك تقتضي مكانة الوقاية من الجريمة في الدستور والقوانين الجنائية الإيرانية أن تراعي المحاكم، عند ممارسة السلطة المقررة في المادة ٢٧، دائما تناسب هذا الحرمان مع الهدف الوقائي المقصود، وأن تتجنب فرض محروميات شاملة وغير ضرورية، وأن توازن في الوقت نفسه بين الآثار الاجتماعية والاقتصادية لقرارها وبين ضرورة حماية المجني عليهم وصون الأمن الاتصالي للمجتمع.[٧]

المطلب الثاني: وضع القواعد المتعلقة بالبيانات والخصوصية والتقنيات الحديثة

تعد المادة ٣٢ من قانون الجرائم المعلوماتية الصادر سنة ١٣٨٨ نقطة مركزية في القواعد الإيرانية المتعلقة بالبيانات والخصوصية والتقنيات الحديثة، لأنها من جهة تلزم مقدمي خدمات الوصول بالاحتفاظ ببيانات المرور لمدة لا تقل عن ستة أشهر من تاريخ إنشائها وبمعلومات المستخدمين لمدة لا تقل عن ستة أشهر بعد انتهاء الاشتراك، ومن جهة أخرى تعرف في تبصراتها نطاق هاتين الفئتين من البيانات بصورة واسعة تشمل المصدر، والمسار، والتاريخ، والوقت، ومدة الاتصال وحجمه، ونوع الخدمة، ونوع الخدمة المستخدمة، والإمكانات الفنية، ومدة الانتفاع، والهوية والعنوان وأرقام الاتصال. وبذلك يكتسب حجم هذه البيانات وتنوعها عمليا خصائص البيانات الضخمة، وتصبح قابلة، عند استخدام خوارزميات متقدمة للذكاء الاصطناعي، لكشف أنماط معقدة في السلوك الاتصالي للمستخدمين. ويبدو هذا الالتزام في ظاهره خادما لتسهيل كشف الجرائم المعلوماتية وتعقبها وإمكان تتبع السلوكيات الإجرامية في بيئة التقنيات الحديثة، إلا أنه في مستوى أعمق يمثل الأساس القانوني لتنظيم العلاقة المعقدة بين ضرورة وصول السلطة إلى البيانات من أجل تحقيق الأمن، وضرورة حماية الخصوصية وحريات الاتصال للمستخدمين، ولهذا يحتل مكانة خاصة في تحليل

الطاقات والتحديات القانونية لتطبيق الذكاء الاصطناعي في التنبؤ بالجريمة والوقاية منها.[٨]تتمثل الوظيفة الأولى للمادة ٣٢ من قانون الجرائم المعلوماتية لسنة ١٣٨٨ في إنشاء آلية قانونية لتتبع مسار الاتصال وإسناد السلوك الإجرامي في البيئات القائمة على التقنية؛ وهي بيئات يستطيع فيها الفاعل المجرم أن يختبئ خلف طبقات متعددة من أسماء المستخدمين والعناوين الإنترنتية وشبكات نقل البيانات، بحيث لا يكون من الممكن عمليا التعرف إليه من بين ملايين المستخدمين من دون وجود سلسلة متماسكة من بيانات المرور. ويفضي إلزام مقدمي خدمات الوصول بالاحتفاظ بمصدر الاتصال ومساره وتاريخه ووقته ومدته ونوع الخدمة، في العمل، إلى إنشاء نوع من البصمة الاتصالية التي تتيح للضابطة والمراجع القضائية، من خلال مطابقة البيانات المضبوطة من نظام الضحية مع البيانات المحفوظة لدى مقدم الخدمة، التعرف إلى الحلقات المجهولة في سلسلة النقل، وإسناد السلوك الإجرامي بدرجة مقبولة من اليقين إلى مستخدم أو إلى مجموعة من المستخدمين. وفي غياب مثل هذا الالتزام القانوني، كانت جرائم معلوماتية كثيرة، ولا سيما النفاذ غير المشروع، والإخلال بالبيانات والنظم، والاحتيالات الشبكية، ستواجه طريقا مسدودا في مرحلة الإثبات، وكانت السياسة الجنائية ستغدو عمليا عاجزة أمام هذه الفئة من الجرائم.[٩]فإن السعة الكبيرة لبيانات المرور ومعلومات المستخدمين التي تأمر المادة ٣٢ من قانون الجرائم المعلوماتية لسنة ١٣٨٨ بالاحتفاظ بها تثير أسئلة جدية بشأن حدود الخصوصية في الفضاء القائم على التقنيات الحديثة، لأن هذه البيانات ليست مجرد مجموعة من الأرقام والتواريخ، بل إن تحليلها قادر على تقديم صورة واضحة عن نمط الحياة اليومية، وشبكة العلاقات الاجتماعية، والعادات الاتصالية، وساعات العمل والراحة، والمواقع المكانية، بل وحتى الميول الفكرية والسلوكية للفرد. إن تركيب البيانات المتعلقة بالمصدر والمقصد والوقت والمدة ونوع الخدمة يصنع في الواقع خريطة للحياة الرقمية للمستخدم، وتستطيع النظم الذكية بسهولة، من خلال معالجة هذه الخريطة، أن تستخرج تصنيفات دقيقة ومتعددة الأبعاد للمستخدمين؛ وهي تصنيفات يمكن، عند استعمالها بغير مسؤولية، أن تصبح أساسا للتمييز أو الإقصاء الاجتماعي أو التدخلات غير المبررة. وهذا الواقع نفسه يبرز ضرورة التفسير الضيق للمادة ٣٢ وتصميم ضمانات تكميلية عند استخدام البيانات المخزنة.[١٠]إن الإلزام بالاحتفاظ ببيانات واسعة بموجب المادة ٣٢ من قانون الجرائم المعلوماتية لسنة ١٣٨٨، إضافة إلى تحديات الخصوصية، يضع مسؤوليات ثقيلة في مجال أمن البيانات على عاتق مقدمي خدمات الوصول، رغم أن المادة نفسها لم تتناول هذا البعد بصورة مباشرة. فكل قاعدة بيانات تتضمن معلومات دقيقة عن اتصالات المستخدمين وخصائصهم الهوياتية والفنية تعد هدفا جذابا للمهاجمين، ولمسيئي الاستعمال من الداخل، بل وللفاعلين الاقتصاديين غير الشفافين، ومع غياب تدابير أمنية صارمة يصبح خطر تسرب هذه البيانات وسرقتها خطرا جديا. وفي فضاء تستطيع فيه نظم الذكاء الاصطناعي أن تدمج البيانات المكشوفة مع مصادر أخرى وتحللها، يمكن أن يؤدي كل خرق أمني إلى موجة واسعة من انتهاك الخصوصية، بل وإلى نشوء أسواق غير قانونية للبيانات الحساسة. لذلك يبين تحليل وضع القواعد المتعلقة بالبيانات والتقنيات الحديثة أن المادة ٣٢ وحدها لا تكفي، وأنه ينبغي، في ضوء المبادئ العامة للمسؤولية المدنية والجنائية، فرض التزام بالحماية الفعالة للبيانات وباعتماد معايير فنية وإدارية صارمة على مقدمي الخدمة، حتى لا يتحول الاحتفاظ بالبيانات نفسه إلى عامل لإنتاج انعدام الأمن.[١١]

المطلب الثالث: دور المؤسسات القضائية والشرطية والتنفيذية في استثمار الذكاء الاصطناعي

يتضح دور المؤسسات القضائية والشرطية والتنفيذية في استثمار الذكاء الاصطناعي في السياسة الجنائية الإيرانية عند النظر إلى البنية القانونية المقررة للنظر في الجرائم المعلوماتية، لأن المشرع، من خلال تعيين مراجع متخصصة واشتراط الكفاءة الفنية في القائمين على هذه المراجع، رسم في الواقع نموذجه المرغوب للتعامل مع الأدلة الرقمية والنظم الذكية. فقد ألزمت المادة ٣٠ من قانون الجرائم المعلوماتية لسنة ١٣٨٨ السلطة القضائية بأن تخصص، بحسب الضرورة، شعبة أو شعبا من النيابات والمحاكم العامة والثورية، وكذلك المحاكم العسكرية ومحاكم الاستئناف، للنظر في الجرائم المعلوماتية، ونصت تبصرة المادة نفسها على أن يختار قضاة هذه المراجع من بين من لديهم الإلمام اللازم بشؤون الحاسوب. ويبدو هذا الحكم في ظاهره متعلقا بالتنظيم الداخلي للجهاز القضائي، لكنه في مستوى أعمق يدل على أن الاستثمار المشروع لطاقات الذكاء الاصطناعي والتقنيات الحديثة في عمليات الكشف والتعقيب والوقاية من الجريمة لا يمكن أن يتحقق من دون سلطة قضائية متخصصة ومتمكنة من التقنية، وقد جعل المشرع، لهذا الغرض، إنشاء شعب خاصة واختيار قضاة ملمين بالحاسوب شرطا ابتدائيا.[١٢]تؤدي المؤسسات التنفيذية كذلك في النظام القانوني الإيراني دورا مزدوجا في استثمار الذكاء الاصطناعي للوقاية من الجريمة، لأنها من جهة، بوصفها متولية للبنى الاتصالية والمصرفية والإدارية، ملزمة بتنفيذ المتطلبات القانونية المتعلقة بحفظ البيانات وتأمين النظم، ومن جهة أخرى، بوصفها مستخدمة للنظم التحليلية في إدارة الخطر، تستطيع أن تضع المقترحات والبيانات المنتجة تحت تصرف المؤسسات القضائية والشرطية، ولا سيما أن الكم الكبير من البيانات المتولدة من عمل هذه الأجهزة يعمل عمليا بمنزلة وقود لنظم الذكاء الاصطناعي وأساس لبنى القرار الجنائي الحديثة. ولا يمكن تنفيذ الالتزامات القانونية مثل الاحتفاظ ببيانات المرور ومعلومات المستخدمين لغرض تتبع السلوك الإجرامي وتمكين الاستناد القضائي إلى هذه البيانات من دون تعاون فعال من الأجهزة

التنفيذية المرتبطة بالاتصالات والمالية والخدمات العامة، كما أن دقة هذا التعاون تؤثر مباشرة في جودة استثمار الذكاء الاصطناعي. فإذا سجل الجهاز التنفيذي البيانات بصورة ناقصة أو غير معيارية أو من دون سلسلة توثيقية، فإن نظم التحليل والذكاء الاصطناعي لدى الشرطة والسلطة القضائية ستعمل هي الأخرى على أساس بيانات معيبة، وهذا يقلل دقة التنبؤ والوقاية ويزيد في الوقت نفسه خطر انتهاك حقوق المواطنين. لذلك لا يقتصر دور المؤسسات التنفيذية في هذه البنية على الامتثال للطلبات القضائية، بل يشمل إنشاء بنية بيانات موثوقة وحفظها، وتحمل المسؤولية عن الاستثمار الصحيح أو غير الصحيح لها.[١٣] يمكن تلخيص دور المؤسسات القضائية والشرطية والتنفيذية في استثمار الذكاء الاصطناعي في النظام القانوني الإيراني في ثلاثة محاور. أولا، تضطلع السلطة القضائية، على أساس المادة ٣٠ من قانون الجرائم المعلوماتية، ومن خلال إنشاء شعب متخصصة واختيار قضاة ملمين بشؤون الحاسوب، بمسؤولية التوجيه والرقابة القانونية على استخدام النظم الذكية، وينبغي لها عبر صياغة ممارسات قضائية منسقة أن توضح معايير الاستناد إلى البيانات الرقمية والمخرجات الخوارزمية. ثانيا، يجب على المؤسسات الشرطية، بوصفها المستخدم الرئيس للنظم التحليلية في مستوى الكشف والوقاية، أن تنظم نشاطها في إطار أوامر المراجع القضائية الخاصة ورقابتها، وأن تلتزم عند تصميم نظم الذكاء الاصطناعي واستثمارها بمبادئ مثل الضرورة والتناسب واحترام الخصوصية. ثالثا، توفر المؤسسات التنفيذية، من خلال إنشاء بنى بيانات مطابقة للقانون وضمان أمن هذه البيانات وسلامتها، الأرضية الفنية اللازمة لعمل النظم الذكية بصورة صحيحة، وتتحمل المسؤولية عن كل استخدام خارج الإطار القانوني. وفي هذا التصور، لا يكون استثمار الذكاء الاصطناعي في سياسة الوقاية ثمرة قرار مؤسسة واحدة منفردة، بل نتيجة تفاعل منظم بين ثلاثة أركان، قضائية وشرطية وتنفيذية، ويتوقف نجاحه على أن يؤدي كل ركن دوره مع إدراك متزامن لمقتضيات التقنية ومتطلبات حقوق الإنسان وسيادة القانون.[١٤]

المبحث الثاني: الآليات التنفيذية والمؤسسية لاستخدام الذكاء الاصطناعي في الوقاية من الجريمة

يبدأ بحث الآليات التنفيذية والمؤسسية لاستخدام الذكاء الاصطناعي في الوقاية من الجريمة في النظام القانوني الإيراني من النقطة التي توقع فيها المشرع، لمواجهة الجرائم المعلوماتية والأدلة الإلكترونية، بنية مؤسسية خاصة. فالمادة ٣٠ من قانون الجرائم المعلوماتية لسنة ١٣٨٨ تلزم السلطة القضائية بأن تخصص، بحسب الضرورة، شعبا من النيابات والمحاكم العامة والثورية، وكذلك المحاكم العسكرية ومحاكم الاستئناف، للنظر في الجرائم المعلوماتية، وتشدد تبصرة المادة نفسها على أن يختار قضاة هذه المراجع ممن لديهم الإلمام اللازم بشؤون الحاسوب. ولا يمثل هذا الحكم تنظيما إداريا بسيطا فحسب، بل يدل عمليا على أن السياسة الجنائية الإيرانية قبلت أن النظر في القضايا التي تؤدي فيها البيانات الإلكترونية والنظم الآلية والأدوات الذكية دورا أساسيا يحتاج إلى مؤسسة قضائية متخصصة تستطيع مراقبة حجية الأدلة الفنية وحدود مشروعية استثمار التقنية في مسار الكشف والتعقيب والوقاية، وأن ترفع في الوقت نفسه مستوى تقييم الأدلة الرقمية والتحليل الخوارزمي من خلال التدريب المستمر للقضاة والضابطة والاعتماد على معايير أدق لتقدير هذا النوع من البيانات. وبذلك تتشكل الأرضية المؤسسية اللازمة للنظر في القضايا التي استخدم فيها الذكاء الاصطناعي في ارتكاب الجريمة أو في تصميم الآليات الوقائية، ضمن إطار شعب خاصة وقضاة ملمين بالتقنية، وتخرج عملية اتخاذ القرار في هذا المجال من مستوى الانطباعات العامة وغير الفنية.[١٥] يكشف الجمع بين حكم المادة ٣٠ من قانون الجرائم المعلوماتية والمادة ٢ من لائحة جمع الأدلة الإلكترونية وقابليتها للاستناد أن الآليات التنفيذية والمؤسسية لاستخدام الذكاء الاصطناعي في الوقاية من الجريمة في إيران تقوم على علاقة متبادلة بين المؤسسات الفنية والمراجع القضائية، بحيث يضطر جهاز العدالة الجنائية، مواكبة للتحولات التقنية واعتمادا متزايدا على الأدوات والخبرات العلمية، إلى الابتعاد عن النهج الحسي والتقليدي المحض في كشف الجرائم وتعقيبها. فمن جهة، يلتزم مقدمو خدمات الوصول والاستضافة بتسجيل البيانات والمعلومات اللازمة وحفظها بالجودة وفي المواعيد المقررة، ومن جهة أخرى تستطيع شعب النيابة والمحكمة المتخصصة، اعتمادا على هذه البيانات وإلمامها بالتقنية، أن تستخدم عند اللزوم نظما تحليلية للتعرف إلى أنماط تكرار الجريمة، وتشخيص العناقيد السلوكية عالية الخطورة، وتقييم فاعلية التدابير الوقائية. وفي مثل هذه البنية، لا يستخدم الذكاء الاصطناعي بوصفه أداة ذاتية الحركة، بل ضمن مسار قانوني وقضائي، ولا تستعمل البيانات المنتجة في الميدان إلا بالقدر اللازم لكشف الجريمة والوقاية الموجهة وتقييم الخطر. وهذا الإدماج بين النظم الفنية الملزمة بتسجيل البيانات والمراجع القضائية المتخصصة يوفر طاقة مهمة لتحويل التحليلات القائمة على البيانات إلى أداة لاتخاذ القرار في السياسة الجنائية.[١٦]

المطلب الأول: الطاقات الشرطية والقضائية في تنفيذ نظم التنبؤ بالجريمة

تعد المادة ٢٨ من قانون الجرائم المعلوماتية لسنة ١٣٨٨، من خلال توسيع مدروس للاختصاص الإقليمي للمحاكم الإيرانية، أحد أهم الأسس القانونية لتعزيز الطاقات الشرطية والقضائية في تنفيذ نظم التنبؤ بالجريمة، لأنها تنص صراحة على أنه متى كانت البيانات الإجرامية أو البيانات المستخدمة في ارتكاب الجريمة محفوظة في نظم أو حوامل بيانات موجودة في نطاق سيادة الجمهورية الإسلامية، أو ارتكبت الجريمة عبر قواعد شبكية تحمل

نطاقا وطنيا إيرانيا، أو استهدفت النظم والقواعد المستخدمة أو الخاضعة لسيطرة السلطات والمؤسسات المقدمة للخدمات العامة، كانت المحاكم الإيرانية مختصة بالنظر. ومعنى هذا التوسع أن معيار اتصال الجريمة بإقليم السيادة لم يعد محدودا بالحضور المادي للمرتكب داخل الحدود، بل إن كل صلة فنية وبنيوية بين السلوك الإجرامي وبين البنى البيانية والاتصالية الإيرانية يمكن أن تصبح أساسا للتدخل القضائي. وفي ضوء هذا الفهم، تملك نظم التنبؤ بالجريمة القائمة على الذكاء الاصطناعي، والتي ترتكز أساسا على تحليل بيانات المرور والمحتوى المتبادل والعلاقات بين النظم الداخلية والعابرة للحدود، سندا واضحا لجمع البيانات المرتبطة بالسلوك الإجرامي وتحليلها ورصدها على المستوى الوطني، وتستطيع المؤسسات الشرطية والقضائية، بالاستناد إلى هذا الاختصاص الموسع، تنظيم تصميم هذه النظم وتنفيذها على نحو يكشف بؤر الخطر الرئيسة في الشبكات المتصلة بالبنى الإيرانية ويديرها.[١٧] بما أن ضمان النظام والطمأنينة في الفضاء السيبراني أصبح أحد المحاور الأساسية للمصلحة العامة في المجتمعات المعاصرة، فإن المادة ٢٨ من قانون الجرائم المعلوماتية تتيح للمؤسسات الشرطية، متى حفظت البيانات الإجرامية في نظم تقع في الإقليم الإيراني، حتى لو كان المرتكب قد تصرف من خارج البلاد، أن تجمع هذه البيانات وتحللها بأمر من المراجع القضائية المختصة، وأن تستخرج أنماط تكرار الجريمة واتساعها باستخدام نظم الذكاء الاصطناعي، لأن العجز عن التعرف إلى هذه الأنماط وضبطها قد يضعف الشعور بالعدالة والأمن في المجتمع الافتراضي على نحو يشبه حالة الإفلات من تطبيق القوانين في العالم الواقعي.[١٨] يكشف الشق المتعلق بارتكاب الجريمة ضد النظم والقواعد المستخدمة أو الخاضعة لسيطرة السلطات والمؤسسات المقدمة للخدمات العامة في المادة ٢٨ من قانون الجرائم المعلوماتية بعدا آخر من الطاقات الشرطية والقضائية لتنفيذ نظم التنبؤ بالجريمة. فعندما تستهدف الهجمات المعلوماتية البنى الحيوية للحكم وتقديم الخدمات العامة، مثل النظم الإدارية والضريبية والصحية أو نظم النقل، تتضاعف الحاجة إلى نظم التنبؤ وتحليل الخطر القادرة على توقع الهجمات المحتملة استنادا إلى البيانات السابقة والمؤشرات الأولية. وتصريح القانون باختصاص المحاكم الإيرانية في هذا المجال يعني أن المؤسسات الشرطية تستطيع، بالتنسيق الوثيق مع مديري هذه النظم وتحت رقابة النيابة والمحاكم المختصة، استخدام نظم الذكاء الاصطناعي للرصد الدائم لحركة البيانات، وتحديد السلوكيات غير العادية، وتصنيف التهديدات، واقتراح التدابير الوقائية، من دون خشية التعارض مع قواعد الاختصاص الإقليمي. وفي هذا الإطار، توضع القرارات الشرطية القائمة على التحليل الآلي للبيانات داخل اختصاص قضائي واضح، وتصبح قابلة للتقييم اللاحق من مرجع النظر.[١٩] يوفر توسيع الاختصاص الإقليمي في المادة ٢٨ من قانون الجرائم المعلوماتية طاقة مهمة لاستقرار نظم التنبؤ بالجريمة في إطار التعاون مع المؤسسات الدولية والشرطية في الدول الأخرى، لأنه متى كانت البيانات الإجرامية أو البيانات المستخدمة في ارتكاب الجريمة محفوظة في نظم قائمة في إيران، أو كانت القواعد الشبكية المرتبطة بالنطاق الوطني الإيراني جزءا من سلسلة الارتكاب، استطاعت المؤسسات الشرطية والقضائية الإيرانية، بالاستناد إلى هذه المادة، أن تطلب تبادل البيانات، أو الحفظ العاجل لها، أو التنسيق في تطبيق التدابير الوقائية. وبذلك يكتسب التعامل مع الطلبات المتبادلة أيضا إطارا شفافا لتحديد حدود التعاون، ويصبح تنفيذ الالتزامات الدولية المتعلقة بمكافحة الجرائم التقنية ممكنا من غير عدول عن المعايير الداخلية.[٢٠] لا تتحقق الطاقات الشرطية والقضائية الناشئة عن المادة ٢٨ من قانون الجرائم المعلوماتية في استقرار نظم التنبؤ بالجريمة بصورة كاملة إلا إذا استطاعت المؤسسات المسؤولة إقامة توازن معقول بين توسيع الاختصاص الإقليمي ومتطلبات سيادة القانون والخصوصية. فمن جهة، يتيح اتساع هذا الاختصاص للمحاكم والنيابات، متى ارتكبت الجريمة في بيئة قواعد شبكية تحمل النطاق الوطني الإيراني أو ضمن نظم قائمة في نطاق سيادة الجمهورية الإسلامية، أن تلجأ إلى أدوات الذكاء الاصطناعي لإجراء تحليل شامل للبيانات وتحديد أنماط الخطر بدقة أكبر. ومن جهة أخرى، فإن هذا الاتساع نفسه، إذا طُبق من دون تحديد واضح للضرورة والتناسب والرقابة القضائية على معالجة البيانات، قد يؤدي إلى تدخل مفرط في الخصوصية الاتصالية للمستخدمين وإلى إضعاف الثقة العامة.[٢١]

المطلب الثاني: الفراغات التشريعية والقيود القانونية القائمة

إن هذا الحل يمنع، في إطار المنطق الكلاسيكي للاختصاص المحلي، ضياع القضايا ولا يسمح بأن يؤدي مجرد الغموض في مكان الارتكاب إلى وقف التعقيب الجنائي. غير أن السؤال الرئيس يبرز عندما يطبق هذا النص على حالات الجرائم الناشئة عن نشاط النظم الآلية، والبنى السحابية، والشبكات الموزعة، ونظم التنبؤ القائمة على الذكاء الاصطناعي، لأن نمط تحقق السلوك الإجرامي في هذه المجالات ليس نقطة واحدة، بل سلسلة من الأفعال والمعالجات المتزامنة في عدة بيئات فنية وجغرافية. وتبدو بنية المادة ٢٩ أقرب إلى نموذج تقع فيه الجريمة في نقطة وتكشف في نقطة أخرى، في حين أن الجرائم القائمة على البيانات لا تسمح دائما بفصل واضح بين محل الارتكاب ومحل الأثر ومحل ملاحظة النتيجة. والنتيجة أن المشرع إذا لم يضع قواعد تكميلية لتحديد الاختصاص في الجرائم المتعددة الأماكن والخوارزمية، فإن طاقة هذه المادة على دعم فاعلية التعقيب في الفضاء الافتراضي أمام نظم الذكاء الاصطناعي المعقدة لن تتحقق بصورة كاملة.[٢٢] في الحالات القائمة على الذكاء الاصطناعي، يمكن أن تكون

الجريمة نتيجة تفاعل مجموعة من النظم الآلية وقواعد البيانات والفاعلين البشريين الموجودين في ولايات قضائية مختلفة، وقد يتخذ القرار الرئيس الذي يفضي إلى الضرر في نقطة لا هي محل الكشف ولا هي، بالمعنى التقليدي، محل الوقوع. فعلى سبيل المثال، قد تكون خوارزمية دُربت على خادم خارج البلاد قد طبقت على بيانات أنتجت في عدة دول، منها إيران، فتكون نتيجتها فعلا إجراميا في بيئة خدمة داخل الإقليم الإيراني، بينما تكون البيانات نفسها موضوعا لاستخراج أنماط سلوكية مشتركة بين مجموعة من الجرائم في أزمنة وأماكن مختلفة، وينشأ عن ذلك تسلسل معقد من مسارات إنتاج البيانات ومرورها ومعالجتها يجعل تعيين نقطة جغرافية واضحة أمرا عسيرا. وفي مثل هذه الحالة، تكون العناوين الفنية ومسارات الاتصال ومحل تخزين البيانات موزعة على نحو يجعل تحديد مكان واحد لوقوع الجريمة صعبا أو متعذرا. وتكتفي المادة ٢٩ من قانون الجرائم المعلوماتية بالإحالة البسيطة إلى محل الكشف أو التبليغ، ومن دون أن تقدم معايير تكميلية لتوزيع الاختصاص في هذه الحالات المتعددة الأماكن والقائمة على البيانات، تعالج المسألة عمليا في قالب النموذج التقليدي نفسه، وتتجاوز السؤال عن أي نقطة في سلسلة البيانات والقرار والتنفيذ ينبغي أن تعد محور الاختصاص وأساس التعقيب في الجرائم الناشئة عن نظم التنبؤ الآلية.[٢٣]تنعكس القيود القانونية القائمة في مجال تحديد حدود صلاحيات نظم التنبؤ الآلية بوضوح في حقيقة أن قانون الجرائم المعلوماتية لسنة ١٣٨٨، على الرغم من إشارته إلى كثير من المفاهيم الأساسية مثل البيانات، والنظام الحاسوبي، وبيانات المرور، لم يقدم أي تعريف للنظم ذاتية التعلم، أو الخوارزميات المتعلمة، أو نظم مساعدة القرار الذكية، أو آليات التنبؤ بالخطر.[٢٤]

المطلب الثالث: مدى توافق التطبيقات مع مبادئ القانون الجنائي والإجراءات الجزائية

ينبغي البحث عن مدى توافق تطبيق نظم الذكاء الاصطناعي في التنبؤ بالجريمة والوقاية منها مع مبادئ القانون الجنائي والإجراءات الجزائية، قبل كل شيء، في ضوء قاعدة المسؤولية الشخصية الأساسية التي صرح بها المشرع في المادة ١٤٢ من قانون العقوبات الإسلامي لسنة ١٣٩٢. فبموجب هذه المادة، لا تثبت المسؤولية الجنائية بسبب سلوك الغير إلا إذا كان الشخص مسؤولا قانونا عن أفعال الغير، أو إذا ارتكب تقصيرا في صلته بنتيجة السلوك الذي ارتكبه الغير. ويعلن هذا الحكم صراحة أن إسناد نتيجة سلوك فاعل إلى شخص آخر يحتاج إلى رابطة قانونية في صورة تكليف قانوني أو تقصير في الرقابة والإدارة، ولا يجوز تقرير مسؤولية جنائية لشخص بمجرد أن النتيجة وقعت في نطاق نفوذه أو مصالحه. وفي مجال استخدام نظم الذكاء الاصطناعي في مراحل مختلفة من السياسة الجنائية، من رصد البيانات والتنبؤ بالسلوك الإجرامي إلى اقتراح القرارات القضائية والشرطية، يمثل هذا المعيار الضابط الرئيس لتقدير توافق هذه التطبيقات أو عدم توافقها مع المبادئ الأساسية للقانون الجنائي والإجراءات الجزائية، لأنه لا يسمح بأن تؤدي نتيجة نظام آلي أو مخرجه، بذاته ومن دون إثبات علاقة التقصير والتكليف لدى المتولي البشري، إلى مسؤولية جنائية مستقلة، وبذلك يمنع نشوء نوع من المسؤولية الجنائية عديمة الوجه القائمة على أحكام آلية.[٢٥]يكون استخدام نظم الذكاء الاصطناعي في التنبؤ بالجريمة منسجما مع مبادئ القانون الجنائي والإجراءات الجزائية إذا بقي لهذه النظم دور مساعد واستشاري إلى جانب الحكم البشري، لا بديلا عنه. فالمادة ١٤٢ من قانون العقوبات الإسلامي، بنفيها أي مسؤولية جنائية مستقلة عن سلوك الغير إلا على أساس التكليف القانوني أو التقصير، تؤكد ضمنا أن القرار النهائي في شأن تطبيق التدابير الوقائية أو التعقيب الجنائي أو إصدار الحكم يجب أن يظل منسوبا إلى إرادة المقام البشري وتقديره، وأن يبقى مخرج النظام في حدود أمارة أو دليل يخضع للتقييم. فإذا استخدمت نظم التنبؤ عمليا على نحو يجعل المقام البشري يؤدي مجرد دور مصادقة ظاهرية، فيوقع نتيجة النظام من دون تحليل مستقل، فإن مبدأ شخصية المسؤولية يضعف في الواقع، لأن القرار الحقيقي يكون قد اتخذ في المستوى الفني، ويغدو إسناده إلى المقام البشري ذا طابع شكلي.[٢٦]يمكن عد المادة ١٤٢ من قانون العقوبات الإسلامي حجر الأساس في تقويم مدى توافق تطبيق نظم الذكاء الاصطناعي مع مبادئ القانون الجنائي والإجراءات الجزائية، بمعنى أن كل مشروع للاستفادة من نظم التنبؤ والوقاية يجب أن يصمم على نحو يضمن، أولا، وجود متول بشري محدد دائما له تكليف واضح بالرقابة واتخاذ القرار، وثانيا، وجود آليات موثقة لتسجيل مراحل التحليل والقرار حتى يكون بالإمكان عند الحاجة فحص وجود التقصير أو عدمه، وثالثا، استخدام مخرج النظام بوصفه أحد عناصر الاستدلال القضائي والإداري، لا بوصفه مصدرا مستقلا للمسؤولية أو دليلا قطعيا.[٢٧]

المبحث الثالث: التحليل النقدي والاستشراف القانوني

في التقييم النقدي للطاقة القانونية القائمة لتنظيم تطبيق نظم الذكاء الاصطناعي في التنبؤ بالجريمة والوقاية منها، تكون نقطة البدء هي إعادة قراءة القواعد العامة للمشاركة والاستعانة بالغير في ارتكاب الجريمة في قانون العقوبات الإسلامي لسنة ١٣٩٢، لأن هذه القواعد ترسم الإطار الرئيس لتوزيع المسؤولية بين الفاعلين المتعددين، ولا بد أن يستند تصنيف الأدوار البشرية في تصميم نظم الذكاء الاصطناعي وضبطها واستثمارها إلى هذا الإطار. وتنص المادة ١٢٥ من قانون العقوبات الإسلامي على أن كل من يشارك مع شخص أو أشخاص آخرين في العمليات التنفيذية لجريمة،

وتكون الجريمة مستندة إلى سلوكهم جميعا، يعد شريكا في الجريمة، وتكون عقوبته عقوبة الفاعل المستقل لتلك الجريمة. وفي الجرائم غير العمدية كذلك، إذا كانت الجريمة مستندة إلى تقصير شخصين أو أكثر، عد الجميع شركاء في الجريمة. ويتيح هذا الحكم، في المستوى النظري، تحليل حالات معقدة يعمل فيها فريق من المصممين والمخططين والمديرين والمستثمرين لنظام تنبؤ أو نظام آلي للتعرف إلى الخطر على نحو يكون فيه الضرر أو النتيجة الإجرامية ثمرة تفاعل مجموعة سلوكياتهم، من دون إمكان عزل دور أحدهم وحده بوصفه فاعلا مستقلا.[٢٨]في الجرائم غير العمدية أيضا، يملك الشق الثاني من المادة ١٢٥، الذي يعد الجريمة في حال استناد نتيجتها إلى تقصير شخصين أو أكثر نتاجا لمشاركة الجميع، قدرة نظرية على تغطية كثير من الحالات الناشئة عن خطأ نظم التنبؤ. فعلى سبيل المثال، إذا أدى نظام صمم للوقاية من الجريمة، بسبب اختيار بيانات متحيزة، وضبط غير صحيح لمؤشرات الخطر من جانب المصمم، وإهمال المستثمر في الرقابة على الأداء، وتقصير مقام الرقابة في المراجعة الدورية، إلى تطبيق تدابير تقييدية غير متناسبة ضد فئة من الأفراد، ثم إلى وقوع سلوكيات إجرامية لاحقة، أمكن تصور أن النتيجة الضارة مستندة إلى تقصير عدة أشخاص، وأنهم جميعا يدخلون في دائرة المشاركة غير العمدية. ومع ذلك، فإن غياب ضوابط خاصة بشأن معيار التقصير في استخدام نظم الذكاء الاصطناعي يثير خطر أن يؤدي الاستناد إلى المادة ١٢٥، بدلا من إنشاء نظام، إلى اضطراب في تشخيص المسؤولية؛ ولا سيما أنه في ظل غياب معايير مهنية محددة لتصميم نظم التنبؤ بالخطر واختبارها، وغياب تعليمات صريحة بشأن لزوم توثيق مسار اتخاذ القرار الآلي، يصبح تحديد السلوك الذي ينتقل، في قضية معينة، من مستوى الخطأ المقبول إلى دائرة التقصير الجنائي أمرا عسيرا.[٢٩]

المطلب الأول: الآثار القانونية والاجتماعية لاستخدام خوارزميات التنبؤ بالجريمة

بموجب المادة ١٢٥ من قانون العقوبات الإسلامي، يعد كل من يشارك مع شخص أو أشخاص آخرين في العمليات التنفيذية للجريمة، وتكون النتيجة الإجرامية مستندة إلى سلوكهم جميعا، شريكا في الجريمة، ويحكم عليه بعقوبة الفاعل المستقل. وفي الجرائم غير العمدية أيضا، متى أسندت النتيجة الضارة إلى تقصير شخصين أو أكثر، عد الجميع شركاء في الجريمة. وهذه القاعدة، التي تعرف المشاركة الجنائية على أساس إسناد النتيجة إلى مجموع السلوكيات، تمثل نقطة انطلاق ملائمة لتحليل الآثار القانونية والاجتماعية لاستخدام نظم التنبؤ بالجريمة القائمة على الذكاء الاصطناعي؛ لأن عمليات التصميم والتدريب والنشر والاستثمار في هذه النظم تتوزع بين عدة فاعلين بشريين، ولأن القرار الذي ينسب ظاهريا إلى مخرج حسابي هو في الواقع ثمرة سلسلة من الاختيارات والضوابط الفنية والإدارية في مستويات مختلفة.[٣٠]يظهر الأثر الأول لاستخدام نظم التنبؤ بالجريمة في كيفية تحديد الشركاء وحدود مسؤوليتهم. فإذا دُرب نظام صمم لتقييم خطر ارتكاب الجريمة على بيانات ناقصة أو متحيزة، وإذا ضبطت معايير الخطر على نحو يضع فئة من المواطنين في مرتبة عالية الخطورة لمجرد مكان السكن أو الخلفية الأسرية، وإذا اتخذت المؤسسات الشرطية والقضائية مخرج النظام، من دون تقييم نقدي، أساسا لإصدار قرارات الضمان، أو الرقابة الإلكترونية، أو القيود الوقائية، فإنه عند حدوث نتيجة ضارة لا يجوز إسناد المسؤولية إلى النظام نفسه، بل ينبغي النظر في الدور الذي أداه كل من المصمم، والمدرب، والمدير التنفيذي، والمقام القضائي في العمليات التنفيذية لهذا القرار.[٣١]يمكن أن يؤثر استخدام نظم التنبؤ بالجريمة تأثيرا عميقا في مبادئ مثل الشفافية، وحق الدفاع، وأصل البراءة، وهذا التأثير يترتب عليه آثار قانونية واجتماعية مهمة. فعندما يصدر المقام القضائي قرار ضمان أو قيدا وقائيا على أساس تقييم خطر قدمه نظام ذكي، يكون للمتهم ومحاميه حق معرفة البيانات التي استند إليها هذا التقييم، ومقدار خطئه المحتمل، والأشخاص الذين شاركوا في تصميمه واعتماده. فإذا كانت بنية النظام على نحو لا يتيح تفسير المخرج، واكتفت بعرض رقم للخطر، فإنها تحد عمليا من إمكان ممارسة حق الدفاع في مواجهة المصدر الرئيس للقرار، وهذا يتعارض مع النظرة التقليدية للإجراءات الجزائية التي تفترض إمكان مواجهة الدليل والمنازعة في صحته وسقمه.[٣٢]

المطلب الثاني: تحديات المسؤولية الجنائية والمدنية والإدارية الناشئة عن الخطأ الخوارزمي

ينبغي تحليل إطار مسؤولية الأشخاص المعنوية عن الخطأ الخوارزمي في نظم الذكاء الاصطناعي، قبل كل شيء، في ضوء المادة ٢٠ من قانون العقوبات الإسلامي لسنة ١٣٩٢ وعلاقتها بالمادة ١٤٣ من القانون نفسه؛ إذ إن الشخص المعنوي، وفقا للمادة ١٤٣، لا يعد مسؤولا إلا إذا ارتكبت الجريمة في اتجاه مصالحه وباسمه وبقرار أو تقصير من مديريه وممثليه، وعندئذ تذكر المادة ٢٠ أنواع العقوبات عند ثبوت هذه المسؤولية. وقد نصت المادة ٢٠ على عقوبات مثل حل الشخص المعنوي، ومصادرة الأموال، والمنع من نشاط مهني أو اجتماعي، والمنع من الدعوة العامة لزيادة رأس المال، والمنع من إصدار بعض السندات التجارية، والغرامة، ونشر حكم الإدانة في وسائل الإعلام، كما استثنت في التبصرة تطبيق هذه العقوبات على الأشخاص المعنوية الحكومية والعامة غير الحكومية في موارد ممارسة السيادة.[٣٣]يكشف الاستثناء الوارد في تبصرة المادة ٢٠، الذي يستبعد تطبيق العقوبات المذكورة على الأشخاص المعنوية الحكومية والعامة غير الحكومية في موارد ممارسة السيادة، تحديا آخر في مجال نظم الذكاء الاصطناعي المستخدمة في سياسة الوقاية من الجريمة. فكثير من نظم التنبؤ بالجريمة، أو تقييم خطر التكرار، أو اقتراح التدابير الوقائية،

تستخدمها مؤسسات قضائية وشرطية وأمنية تعد ممارستها مصداقا لممارسة السيادة، وبناء على هذه التبصرة لا يكون الشخص المعنوي الحكومي المستفيد من النظام، عند حدوث خطأ خوارزمي يؤدي إلى سلب الحرية أو المساس بالسمعة أو التمييز البنيوي، معرضا لعقوبات المادة ٢٠. وهذه الحالة يمكن تبريرها من جهة بهدف منع شل المؤسسات السيادية بفعل العقوبات البنيوية، لكنها من جهة أخرى تحمل خطر إيجاد شعور بالحصانة المؤسسية، وتعزز التصور القائل إن الخطأ الخوارزمي عندما ينبثق من نظم حكومية لا يوجه الرد الجنائي إلى البنية نفسها. وفي مثل هذا الإطار، تبرز الحاجة إلى تقوية المسؤولية الجنائية للأشخاص الطبيعيين صانعي القرار داخل هذه المؤسسات، وكذلك إلى توقع آليات مدنية وإدارية للتعويض والمساءلة التأديبية من أجل سد الفراغ الناشئ عن استثناء المادة ٢٠.[٣٤] تتمثل نتيجة مهمة أخرى لإطار المادة ٢٠ من قانون العقوبات الإسلامي في مجال الخطأ الخوارزمي في الآثار الاجتماعية للجزاءات البنيوية على سوق التقنية وعلى الثقة العامة بنظم الذكاء الاصطناعي. فحل شركة تقنية كبرى أو فرض قيود واسعة على نشاطها بسبب أخطاء خوارزمية يمكن، من جهة، أن يرسل رسالة قوية بشأن جدية احترام حقوق الأشخاص وضرورة المسؤولية في تصميم نظم التنبؤ بالجريمة، لكنه قد يؤدي من جهة أخرى إلى زوال خدمات يعتمد عليها آلاف المستخدمين، وإلى ضياع فرص عمل كثيرة، وإلى تقليل الاستثمار في مجال الابتكار.[٣٥]

المطلب الثالث: حلول الإصلاح التشريعي والسياسات المقترحة

تعد المادة ٢١ من قانون العقوبات الإسلامي، التي تجعل مقدار الغرامة المفروضة على الأشخاص المعنوية لا يقل عن ضعف المبلغ المقرر للأشخاص الطبيعيين ولا يزيد على أربعة أضعافه، نقطة انطلاق مهمة للتفكير في حلول الإصلاح التشريعي في مجال استخدام نظم الذكاء الاصطناعي في التنبؤ بالجريمة والوقاية منها، لأن هذه القاعدة تدل على أن المشرع أدرك بصورة صحيحة أن القدرة الاقتصادية وقوة التأثير لدى الأشخاص المعنوية تجعل العقوبة المالية، إذا لم تنظم بما يتناسب مع هذه القدرة، فاقدة لوظيفتها الرادعة. وفي مجال النظم الذكية، التي تصممها وتستثمرها غالبا شركات ومؤسسات مالية ومقدمو خدمات اتصال ومجموعات تقنية كبرى، ينبغي أن يكون هذا المنطق أساس تصميم الرد الجنائي، بمعنى أنه كلما اتسع نطاق استثمار نظام للتنبؤ بالجريمة، واشتدت الآثار المحتملة لخطئه في الحريات وحقوق المواطنين، وجب أن يكون نطاق الغرامة وسائر الجزاءات المالية متناسبا ومقسما إلى طبقات وقابلا للزيادة، حتى لا يكون بالإمكان قبول الخطر الناشئ عن الخطأ الخوارزمي بوصفه مجرد كلفة نشاط يمكن تجاوزها بدفع مبالغ يسيرة.[٣٦] يمكن أن يشكل تطوير آليات التأمين الخاصة بتطبيقات الذكاء الاصطناعي عالية الخطورة مكملا مهما لنظام المسؤولية والعقوبة. فبوسع المشرع أن يلزم الأشخاص المعنوية التي تستخدم النظم الذكية في المراحل الحساسة من العملية الجنائية، مثل التنبؤ بالجريمة، وتقييم خطر التكرار، وتحديد شدة التدابير الوقائية، أو اقتراح نوع الرد الجنائي، بإبرام عقود تأمين من المسؤولية مع شركات التأمين، بحيث يدفع المؤمن جزءا من الأضرار الناشئة عن الخطأ الخوارزمي ضمن حدود التغطية المقررة.[٣٧] ينبغي أن تقترن الاستفادة من طاقة المادة ٢١ من قانون العقوبات الإسلامي لإصلاح نظام الرد على الخطأ الخوارزمي بتقوية المؤسسات التنظيمية وتشجيع التنظيم الذاتي المهني في مجال الذكاء الاصطناعي. ويمكن إنشاء مجالس أو لجان تخصصية مشتركة بين القطاعات تضم ممثلين عن السلطة القضائية، والمؤسسات التنفيذية ذات الصلة، والجماعة العلمية والمهنية الفاعلة في مجال النظم الذكية، وتكون مهمتها صياغة إرشادات تفصيلية بشأن معايير الحيطة المتعارفة، وطرائق اختبار نظم التنبؤ بالجريمة، وضوابط الشفافية والتوثيق، واقتراح الإصلاحات الدورية في القوانين. وعلى الرغم من أن هذه الإرشادات لا تقع في مرتبة القانون، فإنها يمكن أن تكون للمحاكم والمؤسسات الرقابية أساسا لتشخيص التقصير وتحديد مستوى الغرامة، وبذلك تقيم جسرا بين القواعد العامة في المادتين ٢٠ و٢١ وبين الواقع التقني المعقد.[٣٨]

الخاتمة

النتائج

١. أظهر البحث أن الأنظمة القانونية الثلاثة تعترف بالمبادئ الأساسية لسيادة القانون، والكرامة الإنسانية، والخصوصية، والمحاكمة العادلة، بوصفها قيودا عامة على كل استخدام لنظم الذكاء الاصطناعي في السياسة الجنائية، وبذلك فإن تطوير أدوات التنبؤ والوقاية التقنية لا بد أن يقع ضمن إطار هذه المعايير العامة.

٢. أظهر تحليل قوانين الجرائم المعلوماتية، والأدلة الإلكترونية، وقواعد الاختصاص في إيران والعراق أن البنى اللازمة لقبول البيانات والمستندات الإلكترونية وتوسيع الاختصاص الإقليمي في البيئات الشبكية قد توفرت، وأن الأرضية القانونية لاستخدام النظم القائمة على البيانات في كشف الجريمة وتعقيبها والوقاية منها موجودة من هذه الجهة، وإن كانت بصورة متفرقة وغير نظامية.

٣. أظهر بحث النظام الإماراتي أن هذا البلد، من خلال سن قواعد منسقة في مجال حماية البيانات الشخصية، والمعاملات والمستندات الإلكترونية، والعدالة الجنائية الإلكترونية، أنشأ إطارا شبه كامل لمعالجة البيانات، واستخدام الرقابة الإلكترونية، وقبول الهوية والتوقيع الرقميين، وإدماج نظم الذكاء الاصطناعي في الإجراءات الجنائية.

٤. في مستوى المسؤولية، وفر القانون الإيراني، من خلال توقع المسؤولية الجنائية للأشخاص المعنوية وتشديد الغرامة عليهم، طاقة ملائمة نسبيا لإسناد النتائج الضارة الناشئة عن الخطأ الخوارزمي إلى المؤسسات المستثمرة، في حين يعتمد العراق والإمارات بالدرجة الأكبر على مسؤولية المقامات والمتولين البشريين في مقام تصميم النظم الذكية واستعمالها المتعارف.

٥. أظهر التحليل المقارن لقواعد الإثبات أن الأنظمة الثلاثة تضع بين يدي القاضي مرونة لازمة لقبول الأدلة الإلكترونية ونتائج تحليل البيانات بوصفها قرينة، غير أن أيا منها لا يعد المخرج الخوارزمي دليلا قاطعا غير قابل للمناقشة، وتظل الوظيفة النهائية للقاضي في تكوين القناعة الوجدانية محفوظة.

المقترحات

١. يقترح أن يسن في إيران والعراق قانون شامل لحماية البيانات الشخصية بنظرة خاصة إلى المعالجات عالية الخطورة في المجال الجنائي والأمني؛ قانون يتوقع بصورة واضحة المبادئ الأساسية للمشروعية، والضرورة، والتناسب، وتحديد الغرض، وتقليل البيانات إلى الحد الأدنى، وحقوق الوصول والتصحيح والاعتراض وتقييد المعالجة، وأن يعين مؤسسة رقابية مستقلة وقوية لتنفيذه.

٢. من المناسب أن تعتمد الأنظمة القانونية الثلاثة، من خلال سن قواعد خاصة بشأن اتخاذ القرار الآلي في العملية الجنائية، معايير الشفافية الخوارزمية، والإلزام بالتفسير، وتوثيق منطق القرار، وحق طلب المراجعة البشرية، بصورة صريحة في قوانين الإجراءات الجزائية والوثائق الداخلية الداعمة لحقوق الإنسان، حتى تتعزز الثقة العامة باستخدام نظم الذكاء الاصطناعي.

٣. يقترح في إيران والعراق والإمارات أن يقرر، بوصفه التزاما قانونيا للمؤسسات المتولية، إجراء تقييم للأثر في حماية البيانات والحقوق الأساسية قبل نشر كل نظام للتنبؤ أو الوقاية قائم على البيانات الضخمة والتعلم الخوارزمي، وأن توضع نتائج هذه التقييمات في متناول مؤسسات الرقابة، وأن تنشر قدر الإمكان في صيغة تقارير عامة.

٤. من الملائم توقع آليات ملزمة لتعيين مسؤول عن حماية البيانات ومسؤول عن الرقابة على نظم الذكاء الاصطناعي في المؤسسات الشرطية والقضائية والأمنية في الدول الثلاث، على أن يتمتع هؤلاء الأشخاص بقدر نسبي من الاستقلال، وخبرة فنية وقانونية كافية، وصلاحية التقرير المباشر إلى المراجع العليا، وأن يؤدوا دور حلقة الوصل بين التقنية والقانون.

٥. يقترح في الأنظمة الثلاثة تصميم برامج تدريب منتظمة ومتخصصة وتنفيذها للقضاة، وأعضاء النيابة، والضابطة، والمحامين، في مجال الأسس الفنية للذكاء الاصطناعي، وطرائق تحليل البيانات، ومخاطر التمييز الخوارزمي، وطريقة تقييم الأدلة الخوارزمية، حتى تتقوى فعليا قدرة المؤسسات البشرية على ضبط اتخاذ القرار الآلي والسيطرة عليه.

المصادر

١. ابوذری، مهرنوش. «تأثیر هوش مصنوعی در کیفیت تحقیقات جنایی». مطالعات حقوق و امنیت، ١۴٠١.

٢. افسری، نازیلا. «سیاست جنایی ایران در قبال نقض اصل ٢٣ قانون اساسی در تطبیق با حقوق فرانسه». پایان‌نامه کارشناسی ارشد، دانشگاه ارومیه، دانشکده ادبیات و علوم انسانی، ١۴٠٣.

٣. اقنوم، مهسا. «نقش و تأثیر اشتباه بر مسئولیت کیفری با رویکرد قانون مجازات اسلامی جدید». پایان‌نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد تهران مرکزی، دانشکده حقوق، ١٣٩۴.

٤. امیری، سحر. «مبانی کیفرگذاری در قلمرو جرایم غیرعمدی». پایان‌نامه کارشناسی ارشد، دانشگاه تربیت مدرس، دانشکده حقوق، ١٣٩۶.

٥. بابازاده شهرستانی، رقیه. «دوگانه‌سازی سیاست جنایی در مرحله تعقیب کیفری با تأکید بر قانون آیین دادرسی کیفری مصوب ١٣٩٢». پایان‌نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد بندر انزلی، دانشکده علوم انسانی، ١٣٩۶.

٦. بذرافشان، سارا. «جایگاه نظریه سبب غیرمستقیم در حقوق کیفری ایران با تأکید بر مسئولیت کیفری مقامات عمومی و دولتی». پایان‌نامه کارشناسی ارشد، دانشگاه پیام نور استان خراسان رضوی، مرکز پیام نور مشهد، ١۴٠٠.

٧. بیرجندیان، الناز. «سیاست جنایی اسلام در قبال جرایم علیه مالکیت فکری و تطبیق آن با حقوق ایران و انگلستان». رساله دکتری تخصصی، دانشگاه میبد، دانشکده الهیات و معارف اسلامی، ۱۴۰۴.

۸. حاجیلو، افسانه. «تحلیل و بررسی سند ملی هوش مصنوعی و ارائه توصیه‌های سیاستی». مجموعه مقالات نخستین همایش ملی الگوی حکمرانی تمدنی علم و فناوری، ۱۴۰۲.

۹. حیدرپور، حمیدرضا؛ شهانقی، محمد؛ مهرآرا، ژیلا. «کاربرد هوش مصنوعی در جرم‌یابی و تحقیقات جنایی؛ نمونه‌پژوهی قتل‌های سریالی». تمدن حقوقی، زمستان ۱۴۰۲.

۱۰.خلیلی پاجی، عارف؛ احمدی، امیرحسین. «کاربرد هوش مصنوعی در حقوق کیفری بین‌المللی؛ از مسئولیت‌گریزی تا عدالت الگوریتمی». پاییز، ۱۴۰۶.

۱۱.رستمی زابل، بهزاد. «مسئولیت کیفری ناشی از اقدامات هوش مصنوعی مستقل در نظام حقوق کیفری ایران: چالش‌ها و ضرورت‌های قانون‌گذاری». مجموعه مقالات چهاردهمین کنفرانس بین‌المللی و ملی مطالعات مدیریت، حسابداری و حقوق، ۱۴۰۳.

۱۲.زارعی، جواد؛ ستوده، شهلا. «تأثیر هوش مصنوعی در فرآیند دادرسی کیفری». فقه و حقوق نوین، تابستان ۱۴۰۴.

۱۳.زندی، مهدی؛ رفیعی علوی، سید احسان. «امکان‌سنجی مسئولیت کیفری در هوش مصنوعی بر پایه مبانی فلسفی آن». فلسفه حقوق، بهار ۱۴۰۳.

۱٤.سیدهاشمی، مهسا؛ خلیلی، زهراسادات. «امکان‌سنجی مسئولیت کیفری هوش مصنوعی با تأکید بر شخصیت مستقل حقوقی». عدلیه، زمستان ۱۴۰۳.

۱۵.شیخوند، محمدصادق؛ کردعلیوند، روح‌الدین؛ مینایی، بهروز؛ آشوری، محمد؛ مهدوی ثابت، محمدعلی. «مطالعه تطبیقی کاربرد تسهیل‌کننده هوش مصنوعی در امر تعقیب کیفری؛ ظرفیت‌ها و چالش‌ها». فصلنامه پژوهش‌های حقوق تطبیقی، بهار ۱۴۰۲.

۱٦.صالح‌نژاد بهرستاقی، صابر؛ صوفی، سارا؛ حیدری پرچکوهی، علی. «جرم‌انگاری جرائم نوپدید با بهره‌گیری از هوش مصنوعی». مجله مطالعات حقوق، ۱۴۰۴.

۱۷.صفری، فاطمه؛ زمان‌آبادی، ام‌البنین. «چالش‌های کیفری ناشی از هوش مصنوعی در ارتکاب جرایم سایبری». مطالعات راهبردی علوم انسانی و اسلامی، تابستان ۱۴۰۴.

۱۸.قوامی‌پور، محدثه؛ محمودی، امیررضا. «تأملی بر مسئولیت حقوقی و کیفری ربات‌ها با نگرشی بر نظام برده‌داری در حقوق روم». تحقیقات حقوق خصوصی و کیفری، بهار ۱۴۰۳.

۱۹.کاظم‌پور مشهدی، خلیل. «نگرشی به ابعاد و چالش‌های حقوقی و کیفری هوش مصنوعی». مجموعه مقالات هشتمین کنفرانس بین‌المللی و یازدهمین همایش ملی مدیریت، روان‌شناسی و علوم رفتاری، بی‌تا.

۲۰.کاوه، محمدهادی؛ بارانی، محمد. «مسئولیت کیفری هوش مصنوعی در حقوق کیفری ایران با نگاهی به قوانین اتحادیه اروپا». فقه جزای تطبیقی، پاییز ۱۴۰۳.

۲۱.مجلسی اردجانی، صفورا. «مطالعه عصب‌شناسی از جرم‌شناسی تا حقوق کیفری». پایان‌نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد بندر انزلی، دانشکده علوم انسانی، ۱۴۰۲.

۲۲.محبی بازکیایی، شادی. «بررسی تعدد جرم در فضای مجازی». پایان‌نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد شهر قدس، دانشکده علوم انسانی، ۱۳۹۷.

۲۳.محمدحسینی، بابک؛ قافله‌باشی، سید فهیم؛ هادی‌زاده، مرتضی. «پیشران‌های ارائه خدمات سایبری پایدار در دولت با تأکید بر حفظ امنیت از طریق هوش مصنوعی». آینده‌پژوهی ایران، پاییز و زمستان ۱۳۹۹.

۲٤.محمدی، م. «هوش مصنوعی». نامه فرهنگ، پاییز ۱۳۶۹.

۲۵.معبودیان، فاطمه. «مسئولیت کیفری هوش مصنوعی از دیدگاه حقوق جزا و جرم‌شناسی». مجله علمی و فنی و حقوقی نوین، ۱۴۰۴.

۲٦.مقدر، مهدی. «تحلیل الزامات حقوق عمومی برای تنظیمگری هوش مصنوعی در پیشگیری و کشف جرم». مطالعات علم حقوق، زمستان ۱۴۰۲.

٢٧. هاشمی دمنه، فاطمه سادات؛ حاجی‌آبادی، محمدعلی؛ صالحی، محمد خلیل. «چالش‌های کاربرد هوش مصنوعی در تعیین مجازات: مطالعه تطبیقی حقوق ایران و کامن‌لا». مطالعات حقوق و امنیت، ۱۴۰۴.

هوامش البحث

[١] هاشمی دمنه،فاطمه سادات، محمدعلی، حاجی آبادی، و محمد خلیل، صالحی. «چالش‌های کاربرد هوش مصنوعی در نعیین مجازات: مطالعه تطبیقی حقوق ایران و کامن لا». مطالعات حقوق و امنیت، ۱۴۰۴، ص۳۴۰.

[٢] مهسا؛ خلیلی، زهراسادات؛ سیدهاشمی، ١٤٠٣، امکان‌سنجی مسئولیت کیفری هوش مصنوعی با تأکید بر شخصیت مستقل حقوقی، عدلیه، زمستان ١٤٠٣، شماره ١٠، ص ١٣.

[٣] الناز، بیرجندیان، ١٤٠٤، سیاست جنایی اسلام در قبال جرایم علیه مالکیت فکری و تطبیق آن با حقوق ایران و انگلستان، رساله دکتری تخصصی، دانشگاه میبد، دانشکده الهیات و معارف اسلامی، ص ١٣٨.

[٤] ابوذری، مهرنوش. «تاثیر هوش مصنوعی در کیفیت تحقیقات جنایی». مطالعات حقوق و امنیت، ۱۴۰۱، ص۶.

[٥] شادی، محبی بازکیایی، ١٣٩٧، بررسی تعدد جرم در فضای مجازی، پایان‌نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد شهر قدس، دانشکده علوم انسانی، ص ٢٧.

[٦] هاشمی دمنه،فاطمه سادات، محمدعلی، حاجی آبادی، و محمد خلیل، صالحی. «چالش‌های کاربرد هوش مصنوعی در نعیین مجازات: مطالعه تطبیقی حقوق ایران و کامن لا». مطالعات حقوق و امنیت، ۱۴۰۴، ص۳۴۰.

[٧] صالح نژاد بهرستاقی، صابر، صوفی، سارا، حیدری پرچکوهی، علی، «جرم انگاری جرائم نوپدید با بهره‌گیری از هوش مصنوعی». مجله مطالعات حقوق، ۱۴۰۴، ص۴.

[٨] مهدی مقدر، «تحلیل الزامات حقوق عمومی برای تنظیمگری هوش مصنوعی در پیشگیری و کشف جرم» مطالعات علم حقوق، سال سوم، شماره دوازدهم، زمستان، ۱۴۰۲، ص۹۰.

[٩] معبودیان، فاطمه. «مسئولیت کیفری هوش مصنوعی از دیدگاه حقوق جزا و جرم شناسی». مجله علمی و فنی و حقوقی نوین، ۱۴۰۴،ص ٤

[١٠] مهسا، اقنوم، ١٣٩٤، نقش و تأثیر اشتباه بر مسئولیت کیفری با رویکرد قانون مجازات اسلامی جدید، پایان‌نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد تهران مرکزی، دانشکده حقوق، ص ١٢١.

[١١] صفورا، مجلسی اردەجانی، ١٤٠٢، مطالعه عصب‌شناسی از جرم‌شناسی تا حقوق کیفری، پایان‌نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد بندر انزلی، دانشکده علوم انسانی، ص ٩٦.

[١٢] محمدهادی؛ کاوه، محمد؛ بارانی، ١٤٠٣، مسؤولیت کیفری هوش مصنوعی در حقوق کیفری ایران با نگاهی به قوانین اتحادیه اروپا، فقه جزای تطبیقی، پاییز ١٤٠٣، شماره ١٥، ص ٦.

[١٣] مهدی مقدر، «تحلیل الزامات حقوق عمومی برای تنظیمگری هوش مصنوعی در پیشگیری و کشف جرم» مطالعات علم حقوق، سال سوم، شماره دوازدهم، زمستان، ۱۴۰۲، ص۹۳.

[١٤] بهزاد، رستمی زابل، ١٤٠٣، مسئولیت کیفری ناشی از اقدامات هوش مصنوعی مستقل در نظام حقوق کیفری ایران: چالش‌ها و ضرورت‌های قانون‌گذاری، مجموعه مقالات چهاردهمین کنفرانس بین‌المللی و ملی مطالعات مدیریت، حسابداری و حقوق، ص ٤.

[١٥] عارف خلیلی پاجی، امیرحسین احمدی، «کاربرد هوش مصنوعی در حقوق کیفری بین المللی؛ از مسئولیت گریزی تا عدالت الگوریتمی»، پاییز، ١٤٠٦، ص١٤.

[١٦] محمد صادق شیخوند، روح الدین کرد علیوند ، بهروز مینایی، محمد آشوری، محمد علی مهدوی ثابت، «مطالعه تطبیقی کاربرد تسهیل کننده هوش مصنوعی در امر تعقیب کیفری؛ ظرفیتها و چالشها»، فصلنامه پژوهش های حقوق تطبیقی، دوره ۲۷، شماره ۱، بهار، ۱۴۰۲، ص۸۶.

[١٧] معبودیان، فاطمه. «مسئولیت کیفری هوش مصنوعی از دیدگاه حقوق جزا و جرم شناسی». مجله علمی و فنی و حقوقی نوین، ۱۴۰۴،ص ۷.

[١٨] صالح نژاد بهرستاقی، صابر، صوفی، سارا، حیدری پرچکوهی، علی، «جرم انگاری جرائم نوپدید با بهره‌گیری از هوش مصنوعی». مجله مطالعات حقوق، ۱۴۰۴،ص۹.

[١٩] فاطمه؛ صفری، ام‌البنین؛ زمان‌آبادی، ١٤٠٤، چالش‌های کیفری ناشی از هوش مصنوعی در ارتکاب جرایم سایبری، مطالعات راهبردی علوم انسانی و اسلامی، تابستان ١٤٠٤، شماره ۷۵، ص ۸.

[٢٠] حیدرپور، حمیدرضا، محمد، شهانقی، ژیلا، مهرآرا. «کاربرد هوش مصنوعی در جرم یابی و تحقیقات جنایی؛ نمونه پژوهی: قتل هاب سریالی». مدنیت قانونی، ۱۴۰۲، ص۱۳.

[٢١] معبودیان، فاطمه. «مسئولیت کیفری هوش مصنوعی از دیدگاه حقوق جزا و جرم شناسی». مجله علمی و فنی و حقوقی نوین، ۱۴۰۴،ص ۱۱.

[٢٢] محمدهادی، کاوه، محمد، بارانی. «مسؤولیت کیفری هوش مصنوعی در حقوق کیفری ایران با نگاهی به قوانین اتحادیه اروپا». چکیده، ۱۴۰۲،ص ۸

[٢٣] محمد صادق شیخوند، روح الدین کرد علیوند ، بهروز مینایی، محمد آشوری، محمد علی مهدوی ثابت، «مطالعه تطبیقی کاربرد تسهیل کننده هوش مصنوعی در امر تعقیب کیفری؛ ظرفیتها و چالشها»، فصلنامه پژوهش های حقوق تطبیقی، دوره ۲۷، شماره ۱، بهار، ۱۴۰۲، ص۹۳.

[٢٤] سحر، امیری، ١٣٩٦، مبانی کیفرگذاری در قلمرو جرایم غیرعمدی، پایان‌نامه کارشناسی ارشد، دانشگاه تربیت مدرس، دانشکده حقوق، ص ٥٦.

[٢٥] م، محمدی، ١٣٦٩، هوش مصنوعی، نامه فرهنگ، پاییز ١٣٦٩، شماره ١، ص ٤.

[٢٦] حمیدرضا؛ حیدرپور، محمد؛ شهانقی، ژیلا؛ مهرآرا، ١٤٠٢، کاربرد هوش مصنوعی در جرم‌یابی و تحقیقات جنایی (نمونه‌پژوهی قتل‌های سریالی)، تمدن حقوقی، زمستان ١٤٠٢، شماره ١٨، ص ٦.

[٢٧] افسانه، حاجیلو، ١٤٠٢، تحلیل و بررسی سند ملی هوش مصنوعی و ارائه توصیه‌های سیاستی، مجموعه مقالات نخستین همایش ملی الگوی حکمرانی تمدنی علم و فناوری، ص ۹.

[٢٨] جواد؛ زارعی، شهلا؛ ستوده، ١٤٠٤، تأثیر هوش مصنوعی در فرآیند دادرسی کیفری، فقه و حقوق نوین، تابستان ١٤٠٤، شماره ٢٣، ص ٤.

[٢٩] محدثه؛ قوامی‌پور، امیررضا؛ محمودی، ١٤٠٣، تأملی بر مسئولیت حقوقی و کیفری ربات‌ها با نگرشی بر نظام بردهداری در حقوق روم، تحقیقات حقوق خصوصی و کیفری، بهار ١٤٠٣، شماره ٥٩، ص ٣.

[٣٠] محمدهادی، کاوه، محمد، بارانی. «مسؤولیت کیفری هوش مصنوعی در حقوق کیفری ایران با نگاهی به قوانین اتحادیه اروپا». چکیده، ۱۴۰۲،ص ۱۱

[٣١] محمد صادق؛ شیخوند، بهروز؛ مینایی، محمد؛ آشوری، محمدعلی؛ مهدوی ثابت، روح‌الدین؛ کردعلیوند، ١٤٠٢، مطالعه تطبیقی کاربرد تسهیل‌کننده هوش مصنوعی در امر تعقیب کیفری: ظرفیت‌ها و چالش‌ها، پژوهش‌های حقوق تطبیقی، بهار ١٤٠٢، دوره ٢٧، شماره ١، ص ١٦.

[٣٢] بابک؛ محمدحسینی، سید فهیم؛ قافله‌باشی، مرتضی؛ هادی‌زاده، ۱۳۹۹، پیشران‌های ارائه خدمات سایبری پایدار در دولت با تأکید بر حفظ امنیت از طریق هوش مصنوعی، آینده‌پژوهی ایران، پاییز و زمستان ۱۳۹۹، شماره ۹، ص ۱۷.

[٣٣] رقیه، بابازاده شهرستانی، ١٣٩٦، دوگانه‌سازی سیاست جنایی در مرحله تعقیب کیفری با تأکید بر قانون آیین دادرسی کیفری مصوب ۱۳۹۲، پایان‌نامه کارشناسی ارشد، دانشگاه آزاد اسلامی واحد بندر انزلی، دانشکده علوم انسانی، ص ٩٦.

[٣٤] سارا، بذرافشان، ١٤٠٠، جایگاه نظریه سبب غیرمستقیم در حقوق کیفری ایران با تأکید بر مسئولیت کیفری مقامات عمومی و دولتی، پایان‌نامه کارشناسی ارشد، دانشگاه پیام نور استان خراسان رضوی، مرکز پیام نور مشهد، ص ۲۳.

[٣٥] مهدی؛ زندی، سید احسان؛ رفیعی علوی، ١٤٠٣، امکان‌سنجی مسئولیت کیفری در هوش مصنوعی بر پایه مبانی فلسفی آن، فلسفه حقوق، بهار ١٤٠٣، دوره ۳، شماره ٥، ص ١١.

[٣٦] فاطمه؛ صفری، ام‌البنین؛ زمان‌آبادی، ١٤٠٤، چالش‌های کیفری ناشی از هوش مصنوعی در ارتکاب جرایم سایبری، مطالعات راهبردی علوم انسانی و اسلامی، تابستان ١٤٠٤، شماره ٧٥، ص ١٩.

[٣٧] خلیل، کاظم‌پور مشهدی، بی‌تا، نگرشی به ابعاد و چالش‌های حقوقی و کیفری هوش مصنوعی، مجموعه مقالات هشتمین کنفرانس بین‌المللی و یازدهمین همایش ملی مدیریت، روان‌شناسی و علوم رفتاری، ص ۱۸.

[٣٨] نازیلا، افسری، ١٤٠٣، سیاست جنایی ایران در قبال نقض اصل ۲۳ قانون اساسی در تطبیق با حقوق فرانسه، پایان‌نامه کارشناسی ارشد، دانشگاه ارومیه، دانشکده ادبیات و علوم انسانی، ص ۷۵.