Interdisciplinary Legal Research
Special Issue on Arabic-Language Articles
Sep 2026, 7(4): 288-301
Available online on: www.ilrjournal.ir
e-ISSN:2717-1795

ORIGINAL RESEARCH PAPER

The Preventive Policy towards Artificial Intelligence Crimes

Mohammad Ali Haji Dehabadi*[*1], Mohammad Taleb Mohammad[2]

Abstract

Recent technological advancements, particularly in artificial intelligence (AI), have led to a significant increase in the risks associated with cybercrime, necessitating the development of an effective preventative policy. This policy aims to reduce the occurrence of crimes or mitigate their negative impacts before they happen, through a combination of legal frameworks, technological tools, and social measures. Its importance lies in its ability to protect society from the harmful uses of AI, ensure the accountability of individuals and institutions, and foster trust in modern technology. This study examines the nature of AI-related crimes, encompassing both crimes where AI is used as a tool and crimes committed independently by AI. It focuses on the legal challenges posed by the difficulty in establishing criminal liability and the rapid pace of technological development compared to the lag in legislation. The study also explores preventative tools, including enacting new laws or amending existing ones, and utilizing technical monitoring, awareness campaigns, and training to mitigate risks. The findings indicate that the success of a preventative policy requires the integration of legal, technological, and social aspects, while addressing the ethical and social challenges related to surveillance and privacy protection. Furthermore, the study underscores the need for continued research to develop more effective mechanisms to keep pace with the rapid advancements in AI.

Keywords:
Preventive Policy, AI Crimes, Legal Regulations, Technical Oversight, Criminal Liability, Awareness, Technological Innovation.

1[*] Assistant Professor, Faculty of Law, University of Qom, Qom, Iran.

2 PhD Student, Faculty of Law, University of Qom, Qom, Iran.

Please Cite This Article As: Haji Dehabadi, MA & Taleb, M (2026). "The Preventive Policy towards Artificial Intelligence Crimes". *Interdisciplinary Legal Research*, 7(4): 288-301.

This is an open access article distributed under the terms of the Creative Commons Attribution (CC BY 4.0)

مقاله بحثیه

(الصفحه ۲۸۸-۳۰۱)

السیاسه الوقائیة تجاه الجرائم الذکاء الاصطناعي

محمدعلی حاجی ده آبادی*[۱]، محمد طالب محمد[۲]

۱. استاذ المساعد، کلیه القانون، جامعه قم، قم، ایران.

۲. طالب دکتوراه، کلیه القانون، جامعه قم، قم، ایران.

المخلص

شهدت التطورات التکنولوجیة الحدیثة، وبخاصة في مجال الذکاء الاصطناعي، زیادة ملحوظة في المخاطر المرتبطة بالجرائم الإلکترونیة، الأمر الذي استدعی تطویر سیاسة وقائیة فعالة لمواجهتها. تهدف السیاسة الوقائیة إلی الحد من وقوع الجرائم أو تقلیل آثارها السلبیة قبل حدوثها، من خلال الجمع بین التشریعات القانونیة والأدوات التقنیة والإجراءات الاجتماعیة. وتتمثل أهمیة هذه السیاسة في قدرتها علی حمایة المجتمع من الاستخدامات الضارة للذکاء الاصطناعي، وضمان مسؤولیة الأفراد والمؤسسات، بالإضافة إلی تعزیز الثقة في التکنولوجیا الحدیثة. وتتناول الدراسة طبیعة جرائم الذکاء الاصطناعي، التي تشمل الجرائم التي یستخدم فیها الذکاء الاصطناعي کأداة، والجرائم التي ینفذها الذکاء الاصطناعي بشکل مستقل، مع الترکیز علی التحدیات القانونیة التي تواجه صعوبة تحدید المسؤولیة الجنائیة، وسرعة تطور التکنولوجیا مقارنة بتأخر التشریعات. کما تستعرض الدراسة الأدوات الوقائیة، من ضمنها وضع قوانین جدیدة أو تعدیل القوانین القائمة، واستخدام الرقابة التقنیة والتوعیة والتدریب لتقلیل المخاطر. وتشیر النتائج إلی أن نجاح السیاسة الوقائیة یتطلب تکاملا بین الجانب القانوني والتقني والاجتماعي، مع مراعاة التحدیات الأخلاقیة والاجتماعیة المرتبطة بالمراقبة وحمایة الخصوصیة. کما تؤکد علی ضرورة استمرار البحوث لتطویر آلیات أکثر فعالیة لمواکبة التطور السریع في مجال الذکاء الاصطناعي.

الکلمات المفتاحیة: السیاسة الوقائیة، جرائم الذکاء الاصطناعي، التشریعات القانونیة، الرقابة التقنیة، المسؤولیة الجنائیة، التوعیة، الابتکار التکنولوجي.

المقدمه

شهد العالم في العقود الأخيرة تحولا جذريا في جميع مناحي الحياة بفعل التقدم التكنولوجي السريع، ولا سيما في مجال الذكاء الاصطناعي الذي أصبح جزءا لا يتجزأ من الحياة اليومية، سواء في القطاع الصناعي أو الطبي أو التعليمي أو الأمني. هذه الثورة الرقمية لم تؤد إلى تحسين الإنتاجية ورفع كفاءة الأداء فحسب، بل فتحت أيضا أفقا واسعا للجرائم التي يمكن أن ترتكب باستخدام التكنولوجيا المتقدمة، أو تلك التي ينفذها الذكاء الاصطناعي بشكل مستقل، ما يجعلها أكثر تعقيدا وصعوبة في التتبع والمراقبة مقارنة بالجرائم التقليدية. وقد أضحى من الواضح أن الاعتماد على التشريعات التقليدية وحدها لم يعد كافيا لمواجهة هذه الظاهرة الجديدة، مما استدعى تطوير سياسات وقائية متكاملة تركز على منع وقوع الجرائم أو الحد من آثارها قبل حدوثها، من خلال دمج الأطر القانونية مع الأدوات التقنية والاجتماعية.

السياسة الوقائية في هذا السياق لا تقتصر على اتخاذ إجراءات ردعية بعد وقوع الجريمة، بل تسعى إلى التنبؤ بالمخاطر المحتملة ووضع آليات للحد منها. وتشمل هذه السياسة مجموعة من الإجراءات المتكاملة، بدءا من سن قوانين وتشريعات محدثة تتناسب مع طبيعة جرائم الذكاء الاصطناعي، مرورا بتطبيق الرقابة التقنية المتقدمة، وانتهاء ببرامج التوعية والتدريب للأفراد والمؤسسات، لضمان التزامهم بالمعايير القانونية والأخلاقية في استخدام التكنولوجيا الحديثة. وتبرز أهمية هذه السياسة الوقائية في كونها تحمي المجتمع من الأضرار المادية والمعنوية التي قد تنجم عن الاستخدام غير المشروع للذكاء الاصطناعي، كما تسهم في تعزيز الثقة في التكنولوجيا الرقمية، وهو عامل أساسي في استمرار الابتكار والاستثمار في هذا المجال الحيوي.

تتميز جرائم الذكاء الاصطناعي بخصوصيات تجعل مواجهتها تحديا كبيرا، فهي قد تتخذ شكل جرائم إلكترونية تقليدية باستخدام الذكاء الاصطناعي كأداة، أو قد تنشأ عن أنظمة ذكاء اصطناعي تعمل بشكل مستقل وتتخذ قرارات تؤدي إلى نتائج إجرامية دون تدخل مباشر من البشر. وتطرح هذه الظاهرة أسئلة قانونية معقدة، أبرزها تحديد المسؤولية الجنائية، خصوصا عند غياب الإرادة البشرية المباشرة أو عند استخدام الذكاء الاصطناعي بواسطة أطراف متعددة، مما يثير ضرورة تطوير أطر قانونية جديدة أو تعديل القوانين القائمة لتواكب هذا التطور التكنولوجي. إضافة إلى ذلك، يواجه المشرع تحديا في مواكبة سرعة تطور التكنولوجيا بالمقارنة مع بطء عملية سن القوانين، ما يجعل بعض الجرائم الإلكترونية في فضاء الذكاء الاصطناعي شبه خارج نطاق القانون التقليدي.

ومن جهة أخرى، تعتمد السياسة الوقائية على الأدوات التقنية كعنصر أساسي، حيث يتم توظيف نظم الذكاء الاصطناعي نفسها لرصد الأنشطة المشبوهة أو التنبؤ بالتهديدات قبل وقوعها، بما يتيح للأجهزة الأمنية التدخل المبكر وتقليل الضرر المحتمل. إلى جانب ذلك، فإن الجانب الاجتماعي والثقافي لا يقل أهمية، حيث يشكل الوعي الرقمي والتدريب المستمر للعاملين في المؤسسات العامة والخاصة حجر الأساس في تطبيق السياسة الوقائية بفعالية. إذ لا يمكن لأي تشريع أن يكون نافذ المفعول دون دعم مجتمعي وثقافي يعزز الالتزام بالقوانين والمعايير الأخلاقية، ويشجع على استخدام التكنولوجيا بشكل مسؤول.

كما أن هناك تحديات أخلاقية مهمة تتعلق بالسياسة الوقائية، أبرزها موازنة الأمن مع الحرية وحقوق الخصوصية، فزيادة الرقابة التقنية قد تؤدي إلى شعور الأفراد بانتهاك خصوصيتهم، بينما ضعف الرقابة يترك المجال للجرائم الرقمية للتفشي بشكل أسرع. لذلك، يتعين على صناع القرار وضع معايير دقيقة تحافظ على التوازن بين حماية المجتمع وتشجيع الابتكار التكنولوجي. هذه المعادلة المعقدة تتطلب تعاونا مستمرا بين القانونيين، والمهندسين، والخبراء في الذكاء الاصطناعي، بالإضافة إلى الجهات التعليمية والإعلامية لتشكيل بيئة شاملة للوقاية.

وبناء على ذلك، تبرز الحاجة إلى تبني سياسة وقائية شاملة تتكامل فيها التشريعات القانونية الحديثة مع الحلول التقنية والوعي المجتمعي، بحيث تصبح أدوات الوقاية فعالة وقادرة على الحد من جرائم الذكاء الاصطناعي، سواء تلك المرتكبة باستخدام هذه التقنية كأداة أو تلك التي ينفذها النظام الذكي بشكل مستقل. كما تشدد هذه السياسة على استمرارية البحث العلمي والتطوير لمواكبة التطور المستمر في هذا المجال، الأمر الذي يجعلها سياسة ديناميكية تتكيف مع المستجدات التقنية والتحديات الجديدة. في ضوء هذه المعطيات، تهدف الدراسة إلى استكشاف أبعاد السياسة الوقائية تجاه جرائم الذكاء الاصطناعي، وتحليل الأدوات القانونية والتقنية والاجتماعية المتاحة لتطبيقها، فضلا عن استعراض التحديات والمعوقات التي قد تواجه تنفيذ هذه السياسة، مع تقديم توصيات عملية لتعزيز فعاليتها.

بيان المسالة

تشكل الجرائم المرتبطة بالذكاء الاصطناعي أحد أبرز التحديات القانونية والأمنية التي تواجه المجتمعات الحديثة نتيجة التطور التكنولوجي السريع وانتشار تطبيقات الذكاء الاصطناعي في مختلف المجالات. فبينما يسهم الذكاء الاصطناعي في تحسين الأداء وزيادة الإنتاجية، فإن استخدامه بشكل غير مشروع أو استغلاله من قبل الأفراد أو المؤسسات لأغراض إجرامية يؤدي إلى أضرار مادية ومعنوية كبيرة، تشمل الاختراقات الإلكترونية، الاحتيال المالي، التلاعب بالمعلومات، وحتى الجرائم التي تنفذ بشكل مستقل عبر أنظمة ذكية.

وتنبع المشكلة الرئيسة من التحديات المتعددة التي يفرضها هذا النوع الجديد من الجرائم، والتي تتمثل في صعوبة تحديد المسؤولية القانونية عند استخدام الذكاء الاصطناعي، وغياب الإطار التشريعي الكافي لمواكبة سرعة تطور التكنولوجيا، إضافة إلى محدودية أدوات الرقابة التقنية والوعي المجتمعي بالمخاطر المحتملة. كما أن هناك تحديات أخلاقية واجتماعية تتمثل في ضرورة موازنة الأمن مع حماية الخصوصية وحرية الابتكار، ما يزيد من تعقيد مهمة المشرع وصناع القرار في تصميم سياسات فعالة للوقاية.

من هذا المنطلق، تطرح الدراسة السؤال الأساسي :**كيف يمكن وضع سياسة وقائية فعالة لمواجهة جرائم الذكاء الاصطناعي، بحيث تتكامل فيها الأطر القانونية والتقنية والاجتماعية لمواجهة التحديات الحالية والمستقبلية؟**، إضافة إلى تحديد مدى فعالية التدابير الوقائية المتاحة، والتعرف على أبرز العقبات التي قد تحد من تطبيقها على أرض الواقع.

تهدف هذه الدراسة إلى تقديم تصور شامل للسياسة الوقائية تجاه جرائم الذكاء الاصطناعي، من خلال استكشاف الأدوات القانونية والتقنية والاجتماعية، وتحليل التحديات والمعوقات، مع اقتراح توصيات عملية لتعزيز قدرة المجتمع على مواجهة هذه الجرائم بطريقة متكاملة وفعالة.

اهمية البحث و اهدافه

أهمية البحث

تكتسب دراسة السياسة الوقائية تجاه جرائم الذكاء الاصطناعي أهمية كبيرة على المستويين العلمي والعملي، نظرا للتطور السريع لتكنولوجيا الذكاء الاصطناعي وانتشار استخداماتها في مختلف القطاعات، مما يزيد من احتمالات استغلالها في ارتكاب جرائم معقدة ومتجددة. وتتمثل أهمية البحث في عدة جوانب رئيسية:

1. **أهمية قانونية وتشريعية :**يسعى البحث إلى تسليط الضوء على الفجوات التشريعية القائمة في مواجهة جرائم الذكاء الاصطناعي، وتقديم مقترحات لتعزيز الأطر القانونية لمواكبة التطور التكنولوجي، بما يضمن تحديد المسؤولية القانونية بوضوح وفعالية.
2. **أهمية أمنية ومجتمعية :**يساهم البحث في تعزيز حماية المجتمع من المخاطر المرتبطة بالجرائم الرقمية، وتقليل الأضرار المادية والمعنوية الناتجة عن الاستخدام غير المشروع للذكاء الاصطناعي.
3. **أهمية تقنية :**يوفر البحث دراسة للأدوات التقنية والرقابية التي يمكن توظيفها في الكشف المبكر عن الجرائم ومنع وقوعها، مما يعزز فاعلية السياسات الوقائية.
4. **أهمية علمية وأكاديمية :**يضيف البحث إلى المكتبة العلمية دراسة تحليلية متكاملة حول السياسة الوقائية للجرائم المرتبطة بالذكاء الاصطناعي، مما يسهم في تطوير المعرفة القانونية والتقنية المتعلقة بهذا المجال المستجد.

أهداف البحث

يهدف البحث إلى تحقيق مجموعة من الأهداف الرئيسية التي توجه الدراسة، ومن أبرزها:

1. تحليل طبيعة جرائم الذكاء الاصطناعي وخصائصها القانونية والتقنية والاجتماعية.
2. استعراض السياسات الوقائية القائمة، وتشخيص مدى فعاليتها في مواجهة هذه الجرائم.
3. تحديد الأدوات القانونية والتقنية والاجتماعية التي يمكن توظيفها لتعزيز الوقاية والحد من المخاطر.
4. الكشف عن التحديات والمعوقات التي تعيق تطبيق السياسات الوقائية على أرض الواقع.
5. تقديم توصيات عملية لتطوير إطار شامل للسياسة الوقائية لمواكبة التطور المستمر في مجال الذكاء الاصطناعي.

منهجية البحث

يعتمد هذا البحث على منهجية علمية متعددة الأدوات، تهدف إلى تقديم دراسة شاملة للسياسة الوقائية تجاه جرائم الذكاء الاصطناعي، من خلال دمج التحليل القانوني بالنظرة التقنية والاجتماعية. وتقوم منهجية البحث على المحاور التالية:

1. **المنهج الوصفي التحليلي :**يستخدم هذا المنهج لوصف الظاهرة محل الدراسة، وتحديد خصائص جرائم الذكاء الاصطناعي وأبعادها القانونية والاجتماعية والتقنية. ويتيح المنهج التحليلي فهم العلاقات بين عناصر السياسة الوقائية، وتقييم فعالية الأدوات القانونية والتقنية المتاحة.
2. **المنهج المقارن :**يوظف لمقارنة التشريعات والسياسات الوقائية بين الدول المختلفة، بما يمكن من استخلاص أفضل الممارسات والتجارب الناجحة التي يمكن تطبيقها أو تكييفها مع السياق المحلي.
3. **المنهج الاستقرائي :**يستخدم لتحليل البيانات والمعلومات المستمدة من الدراسات السابقة والمراجع الأكاديمية، للوصول إلى استنتاجات عامة حول التحديات والآليات الفعالة للوقاية من جرائم الذكاء الاصطناعي.
4. **المنهج القانوني التحليلي :**يركز على دراسة النصوص القانونية والتشريعات المتعلقة بالجرائم الإلكترونية والذكاء الاصطناعي، وتحليل مدى كفايتها ومرونتها في مواجهة التحديات التقنية الحديثة.

5. **جمع البيانات والمصادر :**يعتمد البحث على مصادر ثانوية موثوقة تشمل المراجع الأكاديمية، الدراسات المحكمة، التشريعات الوطنية والدولية، والتقارير الصادرة عن المنظمات المتخصصة في التكنولوجيا والأمن السيبراني. كما يتم الاستعانة بالمقالات العلمية والبحوث الميدانية ذات الصلة، لتحليل الاتجاهات الحديثة في تطبيق السياسات الوقائية.

تهدف هذه المنهجية إلى الوصول إلى تصور شامل ومتكامل للسياسة الوقائية تجاه جرائم الذكاء الاصطناعي، مع التركيز على التكامل بين الجوانب القانونية، التقنية، والاجتماعية، وإبراز التحديات والمعوقات، وصولا إلى توصيات عملية قابلة للتطبيق.

المبحث الأول: مفهوم السياسة الوقائية في مواجهة جرائم الذكاء الاصطناعي

المطلب الأول: تعريف السياسة الوقائية وأهميتها

الفرع الأول: تعريف السياسة الوقائية

تعد السياسة الوقائية في مجال القانون الجنائي إحدى الركائز الحديثة التي تستهدف **منع وقوع الجريمة أو الحد من مخاطرها المحتملة**، بدلا من الاقتصار على العقاب بعد وقوعها. فالمفهوم التقليدي للقانون الجنائي كان يركز بشكل رئيسي على استجابة الدولة للجريمة بعد ارتكابها، عبر العقوبة والإصلاح، غير أن التوجه المعاصر يميل إلى ما قبل الحدث، بمعنى **التدخل المبكر** لمنع وقوع الفعل الإجرامي أو تخفيف نتائجه.

ويعرف الباحثون ظاهرة ''منع الجريمة'' بأنها «جهود مجتمعية وقانونية تبذل قبل ارتكاب الجريمة أو في مراحل مبكرة منها، بهدف تخفيض فرص ارتكابها أو تقليص أثرها الضار».[۲]

بعبارة أخرى، السياسة الوقائية هي إطار يحدد المواقف والوسائل القانونية والإجرائية التي تعتمدها الدولة والمجتمع لخفض احتمالية وقوع الجرائم، أو الحد من أضرارها إن وقعت.

من حيث التصنيف، يمكن القول إن السياسة الوقائية تتضمن عناصر عدة: التشريع المخصص أو تعديل التشريعات القائمة لتشمل جوانب الوقاية، التدخل المبكر من خلال برامج تعليمية وتوعوية، والرقابة التقنية والتكنولوجية عند الاقتضاء. كما أنها تستلزم تضافر جهات مختلفة – الجهات التشريعية، التنفيذية، والمجتمعية – في إطار عمل تكاملي.

ومن جهة أخرى، ينبغي التفرقة بين **الوقاية العامة** و**الوقاية الخاصة** من حيث نطاق التطبيق والهدف؛ ففي الوقاية العامة تهدف السياسة إلى حماية المجتمع ككل من المخاطر الإجرامية، عن طريق رفع الوعي، وتحسين الأطر التشريعية، وتعزيز الأمن العام. أما الوقاية الخاصة فتركز على فئات معينة

Al-Rodhan, Nayef R. F. The Impact of Artificial Intelligence on Security and Law Enforcement. Cham: Springer, 2019.

Bassiouni, M. Cherif. Criminal Law and Prevention: Modern Approaches. Leiden: Brill, 2016.

أو مواقع معينة — مثلا برنامج توعوي لمستخدمي الإنترنت أو منظومة حماية تقنية لأحد القطاعات الحيوية. وتبرز هذه الفروق في الأدبيات المعاصرة ضمن إطار ''الوقاية'' في العلوم الجنائية.[1]

بالتالي، إن تعريف السياسة الوقائية لا يقتصر على مفهوم عام، بل يمتد ليشمل **تحديد الأهداف، واختيار الوسائل، وتوزيع الأدوار بين الجهات المسؤولة، وتنفيذها بشكل منهجي**، مع قياس مدى الفاعلية وتقييم النتائج. ويمكن القول إنها تمثل **منظومة عمل وقائية متعددة الأوجه**)تشريعية، تنظيمية، تقنية، تربوية) تهدف إلى تحقيق مستوى أعلى من الأمن المجتمعي وجعل ارتكاب الجرائم أكثر صعوبة.

الفرع الثاني: أهمية السياسة الوقائية تجاه الجرائم الإلكترونية والذكاء الاصطناعي

تتضخم أهمية السياسة الوقائية في ظل التطور التقني السريع وانتشار استخدامات الذكاء الاصطناعي في شتى المجالات، الأمر الذي فتح بدوره آفاقا لإمكانية ارتكاب جرائم عبر هذه التقنية أو بوساطتها. إذ إن جرائم الذكاء الاصطناعي أو المرتبطة به، تعد من الفئة المتجددة والمعقدة – سواء تلك التي تستخدم فيها أنظمة ذكاء اصطناعي كأداة مساعدة أو تلك التي تنفذ من خلال أنظمة ذكية بشكل مستقل — ما يجعل طبيعتها القانونية والتقنية مختلفة عن الجرائم التقليدية.

أولا، من حيث **حماية المجتمع من الأضرار الناتجة عن استخدامات الذكاء الاصطناعي غير القانونية**، فإن هذه الجرائم قد تتسبب في أضرار مادية ضخمة (مثل الاختراقات المالية، التلاعب بالأنظمة الحيوية) وأضرار معنوية (انتهاك الخصوصية، فقدان الثقة في التكنولوجيا). لذلك، تدخل السياسة الوقائية لإيجاد حواجز وقائية، تقلل من فرص وقوع هذه الأفعال قبل وقوعها، عبر ضبط الاستخدامات القانونية، تنظيم المسؤوليات، وتعزيز قدرة الجهات الرقابية والتقنية على كشف المخاطر مبكرا.

ثانيا، من حيث **الحد من الأفعال الإجرامية قبل وقوعها**، فإن التوجه الوقائي يتيح للدولة والمجتمع ألا ينتظرا وقوع الضرر ثم تستجيبا، بل تشرعا في تحليل المخاطر، تجهيز المعايير، وتطبيق التدابير قبل أن تتحول النقطة الحرجة إلى جريمة فعلية. على سبيل المثال، اعتماد تشريعات تقيد استخدامات الذكاء الاصطناعي في أنظمة المراقبة دون ضمان الخصوصية، أو تجهيز برامج توعية لموظفي الشركات الناشئة في حقل الذكاء الاصطناعي، كلها تدابير تمنع أو تقلل من احتمالية ارتكاب الجريمة.

بهذا، تصبح السياسة الوقائية ضرورة متزايدة في عصر الذكاء الاصطناعي، لا خيارا إضافيا، لأن الاعتماد فقط على العقاب بعد ارتكاب الجريمة يتحول إلى استراتيجية غير كافية، لا سيما عندما تكون التقنية سريعة التطور، والمخاطر تتغير بشكل مستمر. كما أن حلول الإبلاغ والإنفاذ بعد وقوع الجريمة غالبا ما تكلف المجتمع كثيرا — ماديا ومعنويا — مقارنة بالتدابير المبكرة.

إضافة إلى ذلك، فإن الوقاية تحقق **عددا من الحصائل الإيجابية** مثل تقليل الخسائر، تعزيز الثقة في الأنظمة التكنولوجية، وتشجيع الابتكار ضمن ضوابط قانونية وأخلاقية واضحة، مما يعزز التنمية المستدامة للتكنولوجيا بدلا من أن تتحول إلى مخاطر مجتمعية.

---

[1] Clarke, Roger. "Preventing Cybercrime: Policies and Practices." Computer Law & Security Review 32, no. 3 (2016): 345–358. https://doi.org/10.1016/j.clsr.2016.03.004

المطلب الثاني: خصائص جرائم الذكاء الاصطناعي

الفرع الأول: طبيعة هذه الجرائم

تتميز جرائم الذكاء الاصطناعي بخصوصيات تجعلها مختلفة عن الجرائم التقليدية، سواء من حيث طريقة التنفيذ أو النتائج المترتبة عليها. ويمكن تصنيفها إلى نوعين رئيسيين:

أولا، **الجرائم التي تستخدم الذكاء الاصطناعي كأداة** .في هذا النوع، يكون الذكاء الاصطناعي مجرد وسيلة مساعدة لارتكاب الجريمة، مثل استخدام أنظمة ذكية للاختراقات الأمنية، الاحتيال المالي، أو سرقة البيانات الرقمية. على سبيل المثال، يمكن استخدام برامج ذكاء اصطناعي لتجاوز أنظمة الحماية في البنوك أو المؤسسات الحكومية، ما يجعل الجريمة أكثر تعقيدا وأقل احتمالا لاكتشافها بسرعة .

ثانيا، **الجرائم التي يتم تنفيذها بواسطة الذكاء الاصطناعي بشكل مستقل**، أي أن النظام الذكي يتخذ قراراته بشكل آلي يؤدي إلى أفعال إجرامية دون تدخل مباشر من البشر. مثال على ذلك: نشر برمجيات ذكاء اصطناعي تتسبب في تعطيل أنظمة البنية التحتية الحيوية أو تلاعب بالمعلومات على نطاق واسع، حيث يقوم النظام الذكي بتنفيذ مجموعة من الأوامر تلقائيا تؤدي إلى نتائج إجرامية .

تظهر هذه الفروقات أهمية فهم طبيعة الجرائم المرتبطة بالذكاء الاصطناعي قبل وضع أي سياسات وقائية، لأن التدابير الوقائية تعتمد على معرفة الطريقة التي يمكن أن يستخدم بها الذكاء الاصطناعي سواء كأداة أو كمنفذ مستقل للجرائم.

الفرع الثاني: التحديات القانونية في مواجهتها

تواجه الدول والجهات التشريعية عدة تحديات عند محاولة مكافحة جرائم الذكاء الاصطناعي، منها ما يتعلق بتحديد المسؤولية القانونية، ومنها ما يرتبط بسرعة تطور التكنولوجيا مقابل بطء التشريعات:

أولا، **صعوبة تحديد المسؤولية الجنائية** .نظرا للطبيعة التفاعلية والمعقدة للأنظمة الذكية، يصبح من الصعب تحديد الشخص أو الجهة المسؤولة عن الجريمة، خاصة إذا كان النظام يعمل بشكل مستقل أو إذا شارك عدة أطراف في تصميم أو تشغيل النظام. فالقانون التقليدي يعتمد على عنصر النية والإرادة البشرية، بينما الذكاء الاصطناعي قد يتصرف بطريقة غير متوقعة، ما يخلق فجوة قانونية .

ثانيا، **سرعة تطور التكنولوجيا مقابل بطء التشريعات** .تتغير أنظمة الذكاء الاصطناعي بسرعة فائقة، بينما تستغرق عملية سن القوانين وتحديثها وقتا طويلا، مما يترك فجوة زمنية يمكن استغلالها من قبل المجرمين. هذا التحدي يفرض على الدول اعتماد سياسات وقائية ديناميكية، تشمل التشريعات المرنة، تطوير أدوات الرقابة التقنية، وبرامج التوعية والتدريب المستمرة .

٤

نايف ر. ف. الرودان، تأثير الذكاء الاصطناعي على الأمن وإنفاذ القانون)شام: سبرينجر، ٢٠١٩)، ص. ٤٥.

ستيفاني غرنوتي–هلي، القوة الإلكترونية: الجريمة والصراع والأمن في الفضاء السيبراني)لندن: روتليدج، ٢٠١٧)، ص. ٧٨.

شريف بسيوني، القانون الجنائي والوقاية: مقاربات حديثة)لايدن: بريل، ٢٠١٦)، ص.١٢٣٣.

ديفيد س. وول، الجريمة الإلكترونية: تحول الجريمة في عصر المعلومات)كامبريدج: بوليتي ڤرس، ٢٠٠٧)، ص. ١١٢.

بناء على ذلك، تتضح أهمية **السياسة الوقائية المتكاملة** التي تجمع بين الجانب القانوني والتقني والاجتماعي، لتقليل فرص ارتكاب هذه الجرائم أو الحد من آثارها. إذ أن الفهم الدقيق لطبيعة الجرائم والتحديات القانونية يمكن صناع القرار من تصميم آليات وقائية فعالة تتوافق مع سرعة تطور التكنولوجيا.

المبحث الثاني: الأدوات والآليات الوقائية لمكافحة جرائم الذكاء الاصطناعي

المطلب الأول: التشريعات والقوانين

الفرع الأول: وضع قوانين جديدة

مع توسع استخدام الذكاء الاصطناعي في مختلف المجالات، أصبح من الضروري وضع **تشريعات جديدة متخصصة** لمراقبة استخدام هذه التكنولوجيا وحماية المجتمع من المخاطر المرتبطة بها. فهذه التشريعات لا تهدف فقط إلى تجريم الأفعال الإجرامية بعد وقوعها، بل تعمل على **تنظيم استخدام الذكاء الاصطناعي بطريقة وقائية**، تحد من استغلاله لأغراض غير قانونية [1].

تشمل هذه التشريعات الجديدة تنظيم **المسؤولية المدنية والجنائية** للأفراد والشركات التي تستخدم أو تطور تقنيات الذكاء الاصطناعي، بحيث يتحمل كل طرف مسؤوليات واضحة تجاه أي أضرار قد تنشأ عن استخدام التكنولوجيا. فعلى سبيل المثال، إذا قام نظام ذكاء اصطناعي طورته شركة معينة بالقيام بأفعال تسبب ضررا للمجتمع أو للأفراد، تكون الشركة مسؤولة عن اتخاذ إجراءات الوقاية، وتعويض المتضررين، وتطبيق العقوبات القانونية عند التقصير [2].

كما يمكن أن تتضمن هذه القوانين وضع قواعد واضحة لاستخدام الذكاء الاصطناعي في الأنشطة الحساسة مثل البنية التحتية الحيوية، النظم المالية، والقطاع الصحي، مع إلزام الشركات والمؤسسات بتطبيق إجراءات أمنية محددة لضمان عدم استغلال الأنظمة الذكية في ارتكاب الجرائم.

الفرع الثاني: تعديل القوانين القائمة

بالإضافة إلى وضع قوانين جديدة، تحتاج الدول أيضا إلى **تحديث القوانين القائمة** لتواكب التطورات التكنولوجية. فعلى سبيل المثال، تعد قوانين الجرائم الإلكترونية التقليدية غير كافية للتعامل مع التعقيدات التي تفرضها الأنظمة الذكية، مثل اتخاذ القرارات بشكل مستقل أو تورط عدة أطراف في عملية واحدة. لذلك، أصبح من الضروري **تعديل نصوص القوانين الحالية لتشمل الذكاء الاصطناعي**، بما يسمح بتطبيقها على الأفعال الإجرامية الحديثة [3].

---

[1] نايف ر. ف. الرودان، تأثير الذكاء الاصطناعي على الأمن وإنفاذ القانون)شام: سبرينجر، ۲۰۱۹)، ص. ۱۰۲.

[2] شريف بسيوني، القانون الجنائي والوقاية: مقاربات حديثة)لايدن: بريل، ۲۰۱٦)، ص.١٤٥.

[3] ستيفاني غرنوتي-هلي، القوة الإلكترونية: الجريمة والصراع والأمن في الفضاء السيبراني)لندن: روتليدج، ۲۰۱۷)، ص. ۸۹.

كما يمكن إدراج **نصوص تتعلق بالوقاية والرصد المبكر**، مثل إلزام الجهات المعنية بإنشاء أنظمة لرصد التهديدات الإلكترونية باستخدام تقنيات الذكاء الاصطناعي نفسها، وتطوير برامج التوعية والتدريب المستمر للمسؤولين القانونيين والأمنيين. فمثل هذه النصوص تساعد على اكتشاف المخاطر قبل أن تتحول إلى أفعال إجرامية، مما يعزز فعالية السياسة الوقائية ويقلل من الأضرار المحتملة .

إن الجمع بين وضع قوانين جديدة وتحديث القوانين القائمة يوفر إطارا قانونيا متكاملا، يتيح **تطبيق سياسات وقائية شاملة**، تجمع بين الوقاية القانونية، الرقابة التقنية، وتعزيز المسؤولية المجتمعية للأفراد والمؤسسات، بما يتماشى مع التطور المستمر في مجال الذكاء الاصطناعي.

المطلب الثاني: الإجراءات الوقائية العملية

الفرع الأول: الرقابة التقنية

تعتبر الرقابة التقنية إحدى الركائز الأساسية في السياسة الوقائية لمكافحة جرائم الذكاء الاصطناعي، حيث يمكن توظيف **نظم الذكاء الاصطناعي نفسها لرصد السلوك الإجرامي** وتحليل الأنماط المشبوهة قبل وقوع الأضرار. فالاعتماد على الذكاء الاصطناعي في الرصد والتحليل يعطي فرصة أكبر للتنبؤ بالتهديدات ومواجهتها بشكل مبكر، مثل اكتشاف محاولات الاختراقات الأمنية أو الأنشطة الاحتيالية عبر الشبكات الرقمية .

علاوة على ذلك، يتم **تطوير أدوات كشف التهديدات والهجمات الإلكترونية** التي تعتمد على تقنيات الذكاء الاصطناعي لتحليل البيانات الضخمة بسرعة ودقة عالية. هذه الأدوات تساعد الجهات الأمنية على التعامل مع الهجمات المعقدة التي قد تتم بشكل مستقل بواسطة الأنظمة الذكية أو بالتعاون بين عدة أنظمة وشبكات، مما يقلل من زمن الاستجابة ويحد من الأضرار المحتملة .

ويمكن تطبيق هذه الرقابة التقنية على مختلف القطاعات الحساسة، مثل البنوك، الطاقة، والمرافق الحيوية، لضمان حماية المجتمع من استغلال الذكاء الاصطناعي في الأغراض الإجرامية، مع ضرورة التحديث المستمر للأنظمة لمواكبة التطور السريع في التكنولوجيا.

الفرع الثاني: التوعية والتدريب

إلى جانب الرقابة التقنية، تشكل **التوعية والتدريب** عنصرا محوريا في السياسة الوقائية، إذ يتيح بناء قدرات بشرية مؤهلة للتعامل مع المخاطر الجديدة للذكاء الاصطناعي. فمثلا، يمكن وضع **برامج توعية للشركات والمؤسسات حول المخاطر** المحتملة، مثل مخاطر تسريب البيانات، الاحتيال الإلكتروني، أو استغلال الأنظمة الذكية في تنفيذ عمليات غير قانونية. وتهدف هذه البرامج إلى تعزيز الوعي لدى المستخدمين والمطورين حول كيفية الحد من الأخطار وتحقيق الاستخدام الآمن للتكنولوجيا .[٤]

مكتب الأمم المتحدة المعني بالمخدرات والجريمة(UNODC) ، دراسة شاملة حول الجرائم الإلكترونية والسياسات الوقائية)فيينUNODC :، ٢٠٢٠(، ص. ٥٦.

نايف ر. ف. الرودان، تأثير الذكاء الاصطناعي على الأمن وإنفاذ القانون)شام: سبرينجر، ٢٠١٩)، ص. ١٢٠.

ستيفاني غرنوتي–هلي، القوة الإلكترونية: الجريمة والصراع والأمن في الفضاء السيبراني)لندن: روتليدج، ٢٠١٧)، ص. ٩٥.

مكتب الأمم المتحدة المعني بالمخدرات والجريمة(UNODC) ، دراسة شاملة حول الجرائم الإلكترونية والسياسات الوقائية)فيينUNODC :، ٢٠٢٠(، ص. ٦٢.

كما يعد **تدريب الأجهزة الأمنية على التعامل مع الجرائم التكنولوجية** ضرورة ملحة، حيث يحتاج العاملون في الأمن الرقمي والشرطة القضائية إلى فهم طبيعة الجرائم الرقمية المعقدة، وكيفية التعامل مع الأدلة الرقمية وتحليلها، واستخدام نظم الذكاء الاصطناعي في التحقيقات. فالتدريب المستمر يضمن سرعة الاستجابة ورفع كفاءة الأجهزة الأمنية في مواجهة التهديدات الإلكترونية الحديثة [1].

إن الدمج بين الرقابة التقنية من جهة، والتوعية والتدريب من جهة أخرى، يوفر **إطارا عمليا متكاملا** للوقاية من جرائم الذكاء الاصطناعي، حيث تعمل الأدوات التكنولوجية على الرصد والتحليل، بينما يضمن العنصر البشري التفاعل الصحيح واتخاذ القرارات الملائمة للتصدي للمخاطر.

المبحث الثالث: التحديات والمعوقات في تطبيق السياسة الوقائية

المطلب الأول: التحديات التقنية والقانونية

الفرع الأول: التحديات التقنية

تواجه سياسة الوقاية من جرائم الذكاء الاصطناعي مجموعة من التحديات التقنية الجوهرية التي تضعف قدرتها على التنبؤ الكامل بالجرائم أو رصدها بكفاءة. أولا، كما أن طبيعة الذكاء الاصطناعي تعد معقدة ومتغيرة باستمرار، فإن **صعوبة التنبؤ بسلوك الذكاء الاصطناعي المعقد** تعد أحد أبرز المعوقات؛ فالأنظمة الذكية قد تتطور أو تغير سلوكها بطرق غير متوقعة، ما يجعل نماذج الرصد والتحليل تفقد فعاليتها بسرعة، أو تصبح غير مناسبة لمواجهة التهديدات الجديدة التي تتجاوز ما كانت مصممة له [2].

ثانيا، هناك **محدودية الأدوات الحالية لرصد الجرائم بشكل كامل**، إذ أن قدرات الكشف والتنبؤ الحالية – رغم التطور التقني – لا تواكب بعد الحجم الهائل للتكنولوجيا، ولا السرعة التي يتم بها ابتكار واستخدام تقنيات الذكاء الاصطناعي لأغراض إجرامية. فعلى سبيل المثال، تدريب خوارزميات على بيانات قديمة أو غير مكتملة يؤدي إلى ظهور «ثغرات» يمكن للمجرمين استغلالها، أو أن تكون هناك أدوات غير قابلة للتكيف مع الاستخدام التلقائي المستقل للذكاء الاصطناعي. هذا ما أكده تحليل حديث الذي يشير إلى أن التحديات التقنية تتضمن دقة الأنظمة، وقابلية البيانات، والشفافية، وغياب المعايير الموحدة لتقييم الأداء الفني للنظم الذكية في البيئة الجنائية [3].

وبالتالي، فإن هذين البعدين التقنيين — عدم القدرة على التنبؤ الكامل، ومحدودية أدوات الرصد — يشكلان عائقا جوهريا في جعل السياسة الوقائية فعالة بشكل كامل. إذ مهما كانت التشريعات والإجراءات، فإن غياب البنية التقنية القادرة على مواكبة التطور السريع يجعل من تنفيذ هذه السياسة غالبا شبه رد فعل بدلا من استباقي.

الفرع الثاني: التحديات القانونية

إلى جانب التحديات التقنية، تواجه السياسة الوقائية أيضا مجموعة من **التحديات القانونية** التي تقوض قدرتها على التطبيق العملي والتحول إلى نتائج ملموسة. أولا، ثمة ما يعرف بـ «غموض المسؤولية القانونية عند استخدام الذكاء الاصطناعي»، فبما أن النظام الذكي قد يتصرف أو يتخذ

---

[1] ديفيد س. وول، الجريمة الإلكترونية: تحول الجريمة في عصر المعلومات)كامبريدج: بوليتي)برس، ۲۰۰۷)، ص. ۱۱۸.

[2] علي، وقار؛ رحمن، تنسيف أور؛ وسعيد، علياء. "الذكاء الاصطناعي في الوقاية من الجرائم والكشف عنها: تعزيز الأمن العام والشرطة التنبؤية ".مجلةASSA ، ۲۰۲۵.

[3] يون، تشيونغ. "التحديات القانونية للذكاء الاصطناعي في مجال الدفاع الجنائي ".ملاحظات المحاضرات في علم النفس التعليمي والإعلام العام، المجلد ۳۰، ۲۰۲۳.

قرارات بشكل مستقل أو شبه مستقل، يصبح من الصعب تحديد من يتحمل المسؤولية: هل هو المطور؟ المستخدم؟ الشركة؟ أو حتى النظام ذاته؟ هذا الغموض يعقد المسارات الجنائية والتعويضية، ويخلق فجوة قانونية تستغل من بعض الجهات للتهرب من المساءلة.

ثانيا، من أبرز المعوقات القانونية هي **التأخر في تحديث التشريعات ومواكبة التطور التقني**؛ فالقدرة التشريعية غالبا تتأخر مقارنة بالسرعة التي تتطور بها تقنيات الذكاء الاصطناعي، ما يترك «فراغا تشريعيا» يمكن أن يستغله المجرمون أو المستخدمون غير القانونيين. وقد بينت بعض الدراسات أن العديد من الأنظمة القانونية لا تزال تفتقر إلى نصوص واضحة تتناول الاستخدام المستقل للذكاء الاصطناعي، أو تلك التي تتناول المسؤولية المدنية والجنائية المرتبطة به، ما يضعف من قدرة القانون على ضبط الواقع الرقمي المتغير.[٢]

من هنا، يظهر أن التحديان القانونيان – الغموض في المسؤولية، وبطء التشريع – يشكلان حجر عثرة أمام الفاعلية الحقيقية للسياسات الوقائية، إذ لا يكفي وجود أدوات تقنية أو برامج رصد، إن لم يكن هناك إطار قانوني واضح يقر ويحدد المسؤوليات ويتيح التنفيذ القضائي أو الإداري.

المطلب الثاني: المعوقات الاجتماعية والأخلاقية

الفرع الأول: المعوقات الاجتماعية

• تعد المعوقات الاجتماعية من أبرز العوامل التي تحد من فعالية تطبيق السياسة الوقائية تجاه جرائم الذكاء الاصطناعي، حيث تلعب مواقف الأفراد والمؤسسات دورا كبيرا في نجاح أو فشل هذه السياسات. أولا، توجد **مقاومة الأفراد والشركات لتطبيق ضوابط صارمة**، خاصة عندما تتطلب تلك الضوابط تغييرات تنظيمية أو استثمارات كبيرة في نظم الرقابة أو تعديل طريقة استخدام الذكاء الاصطناعي. فقد يرى بعض الأفراد أو الشركات أن الإجراءات الوقائية تمثل عبئا أو تقييدا للحرية التشغيلية، ما يؤدي إلى تقليل الالتزام بها أو حتى محاولة الالتفاف عليها .

• ثانيا، يؤثر **الإطار الثقافي الرقمي** على مدى نجاح السياسات الوقائية. فثقافة الاستخدام الرقمي في بعض المجتمعات قد لا تشجع على الالتزام بالقوانين الرقمية أو على التبليغ عن المخالفات، مما يضعف جهود الوقاية. وتشير الدراسات إلى أن الوعي الرقمي، والفهم الأخلاقي للتكنولوجيا، والمستوى التعليمي، كلها عوامل تؤثر على فعالية الإجراءات الوقائية، إذ أن غياب هذه الثقافة يؤدي إلى مقاومة غير مباشرة لتطبيق السياسات .

الفرع الثاني: المعوقات الأخلاقية

• تواجه السياسات الوقائية أيضا تحديات أخلاقية، حيث يجب موازنة **الأمن مع حرية الابتكار** .ففرض قيود صارمة على استخدام الذكاء الاصطناعي لحماية المجتمع قد يعيق الابتكار ويقلل من فرص تطوير تطبيقات جديدة، خاصة في مجالات مثل الرعاية الصحية، التعليم، أو الصناعة. ومن هنا يظهر التحدي الأخلاقي في إيجاد توازن بين حماية المجتمع وبين السماح بالابتكار التقني .

هركي، تشونغور؛ وتوث، دافيد. "الذكاء الاصطناعي في الأمن السيبراني: دراسة المسؤولية، ديناميكيات الجريمة، والاستراتيجيات الوقائيةECLIC ".، ٢٠٢٤.

مكتب الأمم المتحدة المعني بالمخدرات والجريمة .(UNODC) دراسة شاملة حول الجرائم الإلكترونية والسياسات الوقائية .فيينا UNODC :، ٢٠٢٠.

علي، وقار؛ رحمن، تنسيف أور؛ وسعيد، علياء. "الذكاء الاصطناعي في الوقاية من الجرائم والكشف عنها: تعزيز الأمن العام والشرطة التنبؤية ".مجلةASSA ، ٢٠٢٥.

مكتب الأمم المتحدة المعني بالمخدرات والجريمة(UNODC) ، دراسة شاملة حول الجرائم الإلكترونية والسياسات الوقائية)فيينا UNODC :، ٢٠٢٠(، ص. ٦٢.

غرنوتي–هلي، ستيفاني .القوة الإلكترونية: الجريمة والصراع والأمن في الفضاء السيبراني)لندن: روتليدج، ٢٠١٧.(

- إضافة إلى ذلك، يبرز القلق من **المراقبة الزائدة وانتهاك الخصوصية**، إذ يمكن أن تؤدي أنظمة الرصد المستمرة لمراقبة أنشطة الأفراد والشركات إلى شعور بالرقابة المفرطة، وهو ما يثير جدلا أخلاقيا وقانونيا حول الحق في الخصوصية وحماية البيانات. وبالتالي، تحتاج السياسات الوقائية إلى إيجاد حلول متوازنة تضمن الأمن دون المساس بحرية الأفراد وحقوقهم الأساسية [1].
- إن دمج فهم هذه المعوقات الاجتماعية والأخلاقية في تصميم وتنفيذ السياسات الوقائية يعزز من احتمالية نجاحها ويضمن تطبيقها بطريقة متوازنة تراعي جميع الأطراف المعنية.

النتائج

توضح الدراسة أن الجرائم المرتبطة بالذكاء الاصطناعي تمثل تحديا متزايدا للمجتمعات الحديثة، نظرا للطبيعة المعقدة لهذه الأنظمة والسرعة التي تتطور بها التكنولوجيا. ومن خلال تحليل المفاهيم القانونية والتقنية والاجتماعية للسياسة الوقائية، يتضح أن الفعالية الحقيقية للسياسات الوقائية لا تتحقق إلا من خلال **دمج التشريعات الحديثة مع الأدوات التقنية** المتقدمة، حيث تشكل القوانين وحدها أو التكنولوجيا وحدها حلولا ناقصة. فالقوانين توفر الإطار القانوني والرقابي لضمان المساءلة وتحديد المسؤوليات، بينما تمكن الأدوات التقنية من رصد الأنشطة المشبوهة والكشف المبكر عن المخاطر قبل أن تتفاقم إلى جرائم فعلية. هذا التكامل بين القانون والتقنية يتيح استباق الجرائم، ويخفض من الأضرار المادية والمعنوية الناتجة عن استغلال الذكاء الاصطناعي لأغراض غير مشروعة، كما يضمن توافر آليات واضحة للتدخل في الوقت المناسب.

وتظهر الدراسة أن **التوعية والتدريب** يشكلان عنصرا لا يقل أهمية عن التشريع والتقنية، إذ أن البشر هم العامل الحاسم في تنفيذ أي سياسة وقائية. البرامج التوعوية للشركات والمؤسسات والمستخدمين النهائيين ترفع مستوى الوعي بالمخاطر المحتملة وتوضح كيفية التعامل معها، بينما يضمن التدريب المستمر للأجهزة الأمنية والقضائية قدرة هذه الجهات على التعامل مع الجرائم التقنية بكفاءة وفعالية، وفهم طرق تحليل الأدلة الرقمية واستخدام أدوات الذكاء الاصطناعي في التحقيقات. هذه العناصر البشرية تساعد على سد الفجوات التي قد تتركها التشريعات أو التكنولوجيا وحدها، وتدعم الاستجابة الاستباقية بدلا من الاكتفاء بالإجراءات التقليدية بعد وقوع الجريمة.

كما تشير النتائج إلى أن **التحديات التقنية والقانونية والاجتماعية والأخلاقية** تشكل عوائق يجب معالجتها بشكل متكامل، حيث أن غياب التنسيق بين هذه الجوانب يؤدي إلى ضعف الفعالية وارتفاع مخاطر الاستغلال. فالتأخر التشريعي، وغموض المسؤولية القانونية، وسرعة تطور الأنظمة الذكية، وثقافة الاستخدام الرقمي، كلها عوامل تؤثر على مدى نجاح السياسة الوقائية. ومن هنا تظهر أهمية تصميم آليات مرنة تسمح بتعديل التشريعات والتقنيات والإجراءات التدريبية بما يتناسب مع المستجدات، وتضمن التوازن بين الأمن العام وحرية الابتكار والخصوصية الفردية.

وتؤكد الدراسة على الحاجة إلى **استراتيجية شاملة ومتعددة المستويات** للسياسة الوقائية، تشمل وضع قوانين متخصصة، تحديث التشريعات القائمة، توظيف أدوات رصد وتحليل الذكاء الاصطناعي، وبرامج توعية وتدريب فعالة. فتنفيذ مثل هذه الاستراتيجية المتكاملة يقلل من فرص وقوع الجرائم، ويزيد من قدرة المجتمع على حماية بياناته، وأنظمته الحيوية، ومصالحه الاقتصادية، ويحد من الأضرار الناتجة عن أي استخدام غير قانوني للتكنولوجيا.

---

[1] وول، ديفيد س .الجريمة الإلكترونية: تحول الجريمة في عصر المعلومات)كامبريدج: بوليتي برس، ٢٠٠٧.(

وأخيرا، توصي الدراسة بـ **إجراء بحوث مستقبلية** لتطوير آليات قانونية وتقنية متقدمة تتناسب مع سرعة تطور الذكاء الاصطناعي، بما في ذلك ابتكار نظم ذكية للتنبؤ بالتهديدات، وتصميم أطر قانونية مرنة وقابلة للتكيف مع التقنيات الحديثة، واستراتيجيات توعية محدثة باستمرار. كما تشدد على ضرورة دراسة الجوانب الأخلاقية والاجتماعية للسياسات الوقائية لضمان التوازن بين حماية المجتمع وحقوق الأفراد وحريتهم في الابتكار، مما يعزز قدرة الحكومات والمؤسسات على وضع خطط وقائية فعالة ومستدامة في مواجهة جرائم الذكاء الاصطناعي المستقبلية.

المصادر والمراجع

1. ديفيد س. وول، الجريمة الإلكترونية: تحول الجريمة في عصر المعلومات (كامبريدج: بوليتي برس، ٢٠٠٧)، ص. ١١٢.
2. ستيفاني غرنوتي–هلي، القوة الإلكترونية: الجريمة والصراع والأمن في الفضاء السيبراني (لندن: روتليدج، ٢٠١٧)، ص. ٧٨.
3. شريف بسيوني، القانون الجنائي والوقاية: مقاربات حديثة (لايدن: بريل، ٢٠١٦)، ص. ١٢٣.
4. علي، وقار؛ رحمن، تنسيف أور؛ وسعيد، علياء. ‘‘الذكاء الاصطناعي في الوقاية من الجرائم والكشف عنها: تعزيز الأمن العام والشرطة التنبؤية.’’ مجلة ASSA، ٢٠٢٥.
5. غرنوتي–هلي، ستيفاني. القوة الإلكترونية: الجريمة والصراع والأمن في الفضاء السيبراني (لندن: روتليدج، ٢٠١٧).
6. مكتب الأمم المتحدة المعني بالمخدرات والجريمة (UNODC). دراسة شاملة حول الجرائم الإلكترونية والسياسات الوقائية. فيينا: UNODC، ٢٠٢٠.
7. نايف ر. ف. الرودان، تأثير الذكاء الاصطناعي على الأمن وإنفاذ القانون (شام: سبرينجر، ٢٠١٩)، ص. ٤٥.
8. هركي، تشونغور؛ وتوث، دافيد. ‘‘الذكاء الاصطناعي في الأمن السيبراني: دراسة المسؤولية، ديناميكيات الجريمة، والاستراتيجيات الوقائية.’’ ECLIC، ٢٠٢٤.
9. وول، ديفيد س. الجريمة الإلكترونية: تحول الجريمة في عصر المعلومات (كامبريدج: بوليتي برس، ٢٠٠٧).
10. يون، تشيونغ. ‘‘التحديات القانونية للذكاء الاصطناعي في مجال الدفاع الجنائي.’’ ملاحظات المحاضرات في علم النفس التعليمي والإعلام العام، المجلد ٣٠، ٢٠٢٣.
11. Al-Rodhan, Nayef R. F. The Impact of Artificial Intelligence on Security and Law Enforcement. Cham: Springer, 2019.
12. Bassiouni, M. Cherif. Criminal Law and Prevention: Modern Approaches. Leiden: Brill, 2016.
13. Clarke, Roger. “Preventing Cybercrime: Policies and Practices.” Computer Law & Security Review 32, no. 3 (2016): 345–358. https://doi.org/10.1016/j.clsr.2016.03.004