دور الذكاء الاصطناعي في السياسة الجنائية لتنمية الاستدامة (دراسة مقارنة)

م.م. فليحة حسن علي
جامعة بابل/ كلية طب حمورابي
ham833.flyhh.hasan@uobabylon.edu.iq

تاريخ استلام البحث:2026/2/25 **تاريخ قبول النشر:2026/5/11** **تاريخ النشر:2026/6/11**

ملخص البحث: لقد أصبح الذكاء الاصطناعي عنصرًا فاعلًا في تطوير أدوات السياسة الجنائية، من خلال تحليل الأنماط الإجرامية والتنبؤ بمخاطر الجريمة، ودعم أجهزة إنفاذ القانون في عملية اتخاذ القرار، فضلاً عن تحسين كفاءة التحقيقات الجنائية وتعزيز سرعة ودقة الفصل في القضايا. وتكمن أهمية هذا التطور في الانتقال من سياسة جنائية ذات طابع ردّ فعلي إلى سياسة وقائية تستند إلى البيانات والتحليل العلمي

الكلمات المفتاحية: الذكاء الاصطناعي ، البحث الجنائي ، السياسة الجنائية ، التنمية المستدامة

The Role of Artificial Intelligence in Criminal Policy for Sustainable Development

Prepared by

Assistant Lecturer Faliha Hassan Ali
University of Babylon / Hammurabi College of Medicine

Abstract: Artificial intelligence has become an effective element in the development of criminal policy tools by analyzing criminal patterns, predicting crime risks, and supporting law enforcement agencies in the decision-making process, as well as improving the efficiency of criminal investigations and enhancing the speed and accuracy of case resolution.

The significance of this development lies in the transition from a reactive criminal policy to a preventive, data-driven approach grounded in scientific analysis. Artificial intelligence can also contribute to supporting judges' work by analyzing judicial precedents, proposing legal solutions, and assisting in the unification of judicial interpretation, Keywords: Artificial Intelligence, Criminal Investigation, Criminal Policy, Sustainable Development.

Keywords: Artificial Intelligence, Criminal Investigation, Criminal Policy, Sustainable Development

المقدمة

في ظل التحولات الكبرى التي يشهدها العالم المعاصر، برزت ثورة المعلومات بوصفها واحدة من أهم الظواهر الحضارية التي أعادت تشكيل أنماط الحياة الإنسانية على مختلف المستويات الاجتماعية والاقتصادية والثقافية. فقد لم تعد المعرفة حكرًا على نطاق جغرافي محدد، بل أصبحت متاحة بصورة آنية تتجاوز الحدود التقليدية. كما أسهم التطور التقني المتسارع في بناء بيئة تواصلية جديدة تقوم على السرعة والدقة والانتشار الواسع، الأمر الذي أحدث نقلة نوعية في طبيعة التفاعل البشري وفي آليات إدارة شؤون الحياة اليومية.

لقد أفرزت هذه الثورة المعلوماتية واقعًا جديدًا نعيش فيه ضمن شبكة واسعة من الاتصالات الفورية، حيث تنتقل البيانات والمعلومات عبر مسافات شاسعة في لحظات قليلة، ويتم تبادلها على المستويات الدولية والوطنية والمحلية دون عوائق تُذكر. كما أسهمت هذه البيئة الرقمية في تسهيل التعامل مع الأنظمة الحديثة والمتطورة، نظرًا لما توفره من سرعة في إنجاز المعاملات ودقة في الأداء، الأمر الذي عزز من كفاءة المؤسسات ورفع مستوى الإنتاجية في مختلف القطاعات.

مشكلة البحث

في سياق التحولات التقنية المتسارعة وما رافقها من توسّع غير مسبوق في استخدام الوسائط الرقمية، برزت إشكاليات قانونية وأمنية لم تكن معروفة من قبل، الأمر الذي استدعى إعادة النظر في كثير من المفاهيم التقليدية المرتبطة بالجريمة والمسؤولية. فالتطور التكنولوجي، رغم ما يحمله من مزايا، أوجد بيئة جديدة تستلزم معالجة تشريعية وفكرية تتناسب مع طبيعته الخاصة. ومن هنا أصبح من الضروري تحليل الأنماط المستحدثة من الانحرافات المرتبطة بالفضاء الرقمي وفهم خصائصها وتميّزها عن الجرائم التقليدية.

تبرز مشكلة البحث بخطورة هذا النوع من الجرائم بشكل خاص في الاعتداءات التي تطال البيانات والمعلومات المثبتة إلكترونيًا، ومنها جرائم التزوير المعلوماتي، حيث يتم العبث بحقيقة البيانات أو تعديلها بقصد الغش أو التضليل، بما يؤدي إلى إحداث أضرار مادية أو معنوية أو اجتماعية. ويزداد الأمر تعقيدًا نظرًا للطبيعة غير المادية للمعلومة وسهولة نسخها أو تغييرها دون أن يترك ذلك أثرًا محسوسًا كالذي تتركه الجرائم التقليدية.

إن تنامي هذا الشكل الإجرامي يفرض على الأنظمة القانونية تطوير أدواتها التشريعية والرقابية لمواكبة المستجدات التقنية، كما يتطلب تعزيز الوعي المجتمعي بخطورة التعامل غير المشروع مع البيانات الرقمية. فالمسألة لم تعد مجرد إساءة استخدام تقنية، بل أصبحت قضية تمس أمن الأفراد والمؤسسات واستقرار المجتمع ككل في عصر تتصدر فيه المعلومة مكانة محورية في مختلف مجالات الحياة.

اهمية البحث

شهد النصف الثاني من القرن العشرين تحولات تشريعية مهمة رافقت الانتشار المتزايد لاستخدام الحاسبات والأنظمة الرقمية، إذ أدركت الدول مبكرًا أن التطور التقني يستلزم استجابة قانونية تتلاءم مع طبيعته المستحدثة،وتعود البدايات الفعلية لمواجهة الجرائم المعلوماتية إلى تلك المرحلة، حيث تُعد السويد من أوائل الدول التي بادرت إلى سنّ تشريعات خاصة بهذا النوع من الجرائم، ولا سيما ما يتعلق بالتزوير المعلوماتي. فقد صدر قانون البيانات السويدي عام 1973، متناولًا جرائم الدخول غير المشروع إلى البيانات الحاسوبية، أو العبث بها، أو تغييرها، أو الاستحواذ عليها بغير وجه حق. ويُعد هذا التشريع خطوة رائدة في الاعتراف بالمعلومة الرقمية بوصفها محلًا للحماية القانونية.

كما اتجهت المملكة المتحدة إلى تنظيم هذا المجال، فأصدرت قانون مكافحة التزوير والتزييف عام 1986، والذي تضمّن في تعريفاته مفهوم أداة التزوير ليشمل وسائط التخزين الحاسوبية المتعددة، فضلاً عن أي وسيلة يُمكن التسجيل عليها سواء بالطرق التقليدية أو الرقمية أو غيرها من الوسائل التقنية. ويعكس ذلك وعيًا مبكرًا بتطور أدوات الجريمة واتساع نطاقها.

ومن ثمّ يتضح أن التطور التقني لم يسر بمعزل عن الاستجابة التشريعية، بل واكبه جهد قانوني تدريجي هدفه حماية البيانات وضمان أمن المعاملات في البيئة الرقمية الناشئة آنذاك.

منهج البحث

اعتمد البحث الحالي على المنهج القانوني المقارن

خطة البحث

قسم البحث الحالي بمبحثين الاول تضمن ماهية الذكاء الاصطناعي والتنمية المستدامة والمبحث الثاني تضمن الاساس القانوني واجراءات الذكاء الاصطناعي في التحقيق والتنمية المستدامة.

المبحث الأول

ماهية الذكاء الاصطناعي والتنمية المستدامة

تخطط نظم دعم القرار لمعالجة مهمة إدارية أو مشكلة محددة بعينها، ويكون نطاق استخدامها مقتصرًا على هذا الإطار. وقد جرى تطوير هذه النظم أساسًا لخدمة مستويات الإدارة الوسطى والعليا، مع إتاحة إمكانية استفادة الإدارة الدنيا من بعض وظائفها ، ومن هذا المنطلق سنبين ذلك بمطالب:

المطلب الاول

الذكاء الاصطناعي

الذكاء الاصطناعي يعمل على صنع القرارات وإتخاذ القرارات بصفة عامة، إلا أنها تعد ملائمة لخدمة القرارات غير الهيكلية والشبه هيكلية التي يكون من الصعب تحديد احتياجاتها [1، ص117].

تتسم نظم دعم القرار بقدرات تحليلية متقدمة، فضلاً عن اعتمادها على قواعد بيانات داخلية وخارجية. وغالبًا ما تستمد هذه النظم بياناتها الداخلية من نظم تشغيل البيانات ونظم المعلومات الإدارية. كما تمتاز بالمرونة والقدرة على التكيّف مع الاحتياجات المتغيرة للمستخدمين من المعلومات، إذ تُعد نظمًا موجهة نحو المستخدم، ويعتمد تشغيلها على مبادرته في طلب الدعم لعملية اتخاذ القرار. وانطلاقًا من ذلك، توفر هذه النظم لغات استعلام وتقصٍّ مألوفة تسهم في تحقيق سهولة الاستخدام. وتتميز نظم دعم القرار كذلك بطابعها التفاعلي، حيث يتيح التفاعل بين المستخدم والنماذج التحليلية إمكانية تعديل افتراضات التحليل وإعادة معالجتها، بما يؤدي إلى الحصول على نتائج جديدة تدعم عملية اتخاذ القرار [2، ص247].

وتتفاوت نظم تدعيم القرارات في درجة تأثيرها المباشر على القرارات، حيث يقتصر بعضها على توفير المعلومات بطرقة تفاعلية سهلة من واعد البيانات في حين يصل مستوى تدعيم البعض الآخر إلى تقديم اقتراح بالقرار المناسب، حيث أصبحت نظم المعلومات تستند على تكنولوجيا الذكاء الاصطناعي وفيما يأتي سوف نتطرق إلى المفاهيم الأساسية الذكاء الاصطناعي:

– **الذكاء:** عملية معقدة قادرة على تمكين الكائن الحي من التكيف المتجدد الذي يناظر فيه الفكر والعمل على الوسائل والغايات.

– **اصطناعي:** كلمة ترتبط بالفعل يصطنع وبالتالي تطلق الكلمة على كل الأشياء التي تنشأ نتيجة النشاط أو الفعل الذي يتم من خلال اصطناع وتشكيل الأشياء تمييزا عن الأشياء الموجودة بالفعل والموجودة بصورة طبيعية دون تدخل الإنسان.

وبذلك فالذكاء الاصطناعي هو الذكاء الذي يصطنعه الإنسان في الآلة أو الحاسوب، وعائلة الذكاء الاصطناعي في صورتها الراهنة تشير على مجموعة متنوعة من التطبيقات الجديدة في الحقول العلمية والنظرية المختلفة. وبذلك فإن طبيعة هذه العائلة مفتوحة وتستقبل أفرادا جدد وابتكارات ملازمة لاستخدامات غير معروفة سابقا للذكاء الاصطناعي [3، ص248] .

المطلب الثاني

التنمية المستدامة

جاء في قاموس اكسفورد الدقيق السياسي ان التنمية المستدامة هي المفهوم الذي يؤكد التوازن بين مصالح النمو الاقتصادي والحماية البيئية ، ويؤكد أهمية التحويلات بين الأجيال ، والحفاظ على الموارد غير المتجددة والحفاظ على مجموعة متنوعة من المبادئ المحددة بخصوص مسؤوليات صناع القرار [4، ص32] .

وقد ضمت اللجنة ممثلين من الدول المتقدمة والنامية ، وعقدت اجتماعات عامة في دول مختلفة في كل أرجاء العالم .

وكانت اللجنة واضحة في تقريرها حيث لم تضع مسودة تتضمن التفاصيل كافة عن المشاكل الموجودة ، وما هو سبب هذه المشاكل بل قامت بوضع طريقة يكون بإمكان الأفراد في الدول المختلفة من خلالها ان تخلق السياسات والتطبيقات الملائمة

ولقد بينت هذه اللجنة ان التنمية المستدامة تحوي مفهومين رئيسين هما :

- الاحتياجات ، ولا سيما احتياجات الفقراء في العالم ، والفقر يعد تلوثاً للبشر .
- القيود التي أوجدتها التكنولوجيا والتنظيم الاجتماعي بخصوص قدرة البيئة على تلبية كل الاحتياجات الحالية والمستقبلية [5، ص78] .

وبالتالي فان التقرير يتنبأ بإمكانية تحقيق النمو الاقتصادي القائم على أساس السياسات التي تديم ، وتوسع قاعدة الموارد البيئية الطبيعية ، وعلى أية حال فان أكثر أشكال النمو الاقتصادي لها طلبات من البيئة ، من حيث استخدام الموارد الطبيعية التي تكون محددة أحيانا وينجم عن هذا الاستخدام توليد فضلات او تلوث ، وهذا من شأنه ان يعرض نمو الأجيال القادمة للخطر وتحاول فلسفة التنمية المستدامة حل هذه المعضلة بالإصرار على ان تكون القرارات المتخذة على أي مستوى في المجتمع يجب ان تضع أمامها النتائج البيئية المترتبة عليها ، والنمو الاقتصادي الصحيح القائم على أساس التنوع الحيوي ورقابة النشاط المدمر بيئيا ، وتعويض الموارد المتجددة مثل الغابات ، ويمكن لهذه الإجراءات ان تعزز البيئة الطبيعية [6، ص34] .

واختيار نوع النمو الاقتصادي الصحيح القائم على أساس التنوع الحيوي ، ورقابة النشاطات المدمرة بيئيا ، والعمل على إدامة الموارد . [7، ص27] وقد لاحظت اللجنة ان التنمية المستدامة تشتمل على نحو أوسع من النمو الاقتصادي فهي تستوجب تغييرا في طبقة النمو لجعلها أقل مادية ، ومكثفة الطاقة ، ولجعلها أكثر مساواة من حيث أثارها ، ولاحظت اللجنة ان الفكرة المشتركة الاستراتيجية للتنمية المستدامة يجب ان تجعل الاعتبارات الاقتصادية والبيئة مندمجة في عملية صنع القرار ، ولكي يحدث هذا استنتجت اللجنة أنه يجب ان تكون هناك تغيرات في

السلوكيات والأهداف والإجراءات المؤسساتية فضلا عن القوانين ، وعلى كل المستويات ولقد لاحظت اللجنة ان التغيرات في القوانين لوحدها لا تكون كافية لحماية المصالح المشتركة فحماية كهذه تتطلب معرفة المجتمع ودعمه التي استوجبت بدورها المزيد من المشاركة العامة في القرارات حول البيئة والموارد ، من خلال قراءة بعض المؤشرات التي استعرضها كل من Roger and James ، في كتابهما ، يمكن تكوين تفسيرات متعددة لفكرة مفهوم الاستدامة، منها:

1-أ- هي الحالة التي لا تنخفض فيها المنافع بمرور الزمن .

ب- هي الحالة التي لا ينخفض فيها الاستهلاك بمرور الزمن .

2- هي الحالة التي تكون فيها الموارد المدارة بشكل يحفظ فرص الإنتاج المستقبلي .

3- هي الحالة التي لا يخفض فيها أسهم رأس المال الطبيعي بمرور الزمن .

4- هي الحالة التي تكون فيها إدارة الموارد بشكل يحافظ على نتاج خدمات هذه الموارد[8، ص46].

5- هي الحالة التي تلبي بأقل تقدير شروط استقرار النظام الرئيس ومرونته بمرور الزمن

إذ ان النقطة 1 [أ ، ب] تدل على فكرة استدامة الاستهلاك ، وتعني هذه الفكرة ان المنفعة لا تشهد انخفاضا خلال الزمن وكذلك الاستهلاك ، ويمكن ان يطلق على هذه الفكرة فكرة استدامة المنافع او فكرة استدامة الاستهلاك ويمكن عدّ المنفعة والاستهلاك معيارين متكافئين بالامكان معالجتهما لغرض الوصول إلى الاستدامة[9، ص123] .

والنقطة 2 تدل على فكرة إدارة الموارد بشكل يحافظ على فرص الإنتاج في المستقبل وكيفية توزيع الموارد الناضبة خلال الزمن أي ما هو المقدار من موارد العالم الناضبة الذي يستخدمه الجيل الحالي ، وما هو المتبقي الذي يجب تركه للأجيال القادمة . النقطة 3 هي الحالة التي لا تخفض فيها أسهم رأس المال الطبيعي بمرور الزمن وتعبر هذه الفكرة عن ان الاستدامة هي المحافظة على خزين رأس المال الطبيعي من الانخفاض خلال الزمن ويشير بعض الاقتصاديين إلى ان المبدأ شرط أساسي لإدامة واستمرار الناتج الاقتصادي واستمراره

والنقطة 4 يقصد بها إدارة الموارد بشكل يحافظ على نتاج خدمات هذه الموارد أي إدارة الموارد بشكل يديم العطاء المستدام لخدمات الموارد ، فالعطاء المستدام هو الذي يعطي حالة مستقرة يتم فيها المحافظة على خزين رأس المال وبمستوى ثابت ويعطي تدفقا مستمرا وانسيابيا لهذا المورد ، فمثلا الغابة تمثل خزين المورد ، وان هذا المورد يكون مستداما عندما تتم إعادة غرس أشجار بدل المزالة ، وبالتالي سيكون بإمكان الغابة ان تعطي إنتاجا مستمرا من الأخشاب[10، ص67] .

المبحث الثاني

اجراءات الذكاء الاصطناعي وارتفاع الجرائم

في إطار التحليل القانوني للظواهر الإجرامية المستحدثة، يثور التساؤل حول الطبيعة القانونية للجرائم المرتبطة بالفضاء الرقمي ومدى خضوعها للقواعد التقليدية في التشريع الجزائي [11، ص11] .

وتندرج الجرائم المرتكبة عبر الإنترنت، أو ما يُعرف بالجرائم المعلوماتية، ضمن نطاق القانون الجنائي الداخلي (الوطني)، من حيث الأصل، باعتبار أن لكل دولة سلطة تنظيم الأفعال التي تقع داخل إقليمها أو تمس مصالحها الجوهرية. فالمشرّع الوطني هو المختص بتجريم الأفعال وتحديد أركانها وبيان العقوبات المقررة لها، حتى وإن ارتُكبت الوسيلة الإجرامية عبر شبكة عابرة للحدود، غير أن خصوصية هذا النوع من الجرائم تكمن في طبيعته العابرة للإقليم، إذ قد يتم الفعل في دولة، وتتحقق نتيجته في دولة أخرى، أو تُستخدم خوادم موزعة جغرافيًا، مما يثير إشكالات تتعلق بالاختصاص القضائي وتنازع القوانين. تبقى القاعدة أن المعالجة الأولى لهذه الجرائم تتم في إطار التشريع الوطني، على أن يُستكمل ذلك بالتعاون الدولي عند الحاجة، ومن هذا المنطلق جاء المبحث الثاني بمطالب:

المطلب الاول

ارتفاع نسبة الجرائم

نظرًا لحداثة هذا النوع من الجرائم، وما أثاره من إشكالات قانونية معاصرة، فقد أصبح من الضروري الوقوف على حقيقته المفهومية وتحليل أبعاده بدقة.

فالجرائم المرتكبة عبر الإنترنت تُعد من الموضوعات المستحدثة التي برزت بقوة على الصعيدين الوطني والدولي، نتيجة الارتباط الوثيق بينها وبين التطور التقني المتسارع. ومن ثمّ فإن تحديد الطبيعة القانونية الخاصة للجريمة المعلوماتية يقتضي أولًا وضع تعريف واضح لها، وبيان عناصرها المميزة، فضلًا عن تحديد محلها الذي تنصب عليه الحماية الجزائية. ذلك أن خصوصيتها لا تنبع فقط من وسيلتها التقنية، بل من طبيعة الاعتداء الذي يطال البيانات أو الأنظمة أو الشبكات المعلوماتية، الأمر الذي يميزها عن الجرائم التقليدية في بنيتها وأدواتها وآثارها.

ويلاحظ عدم وجود اتفاق على مصطلح معين للدلالة على هذه الظاهرة المستحدثة، فهناك من يطلق عليها الغش المعلوماتي، أو الإختلاس الملعوماتي أو الجريمة المعلوماتية [12، ص43] ، ونظرا لصعوبة إعطاء تعريف لهذه الظاهرة الإجرامية وذلك حصرها في مجال ضيق [13، ص89] .

في سياق الجدل الفقهي حول تحديد مفهوم الجريمة المعلوماتية، برزت اتجاهات متعددة حاولت ضبط هذا المصطلح وفق زوايا مختلفة.

فقد قدّم أحد الخبراء الأمريكيين تصورًا واسعًا لها، إذ اعتبرها كل سلوك إجرامي عمدي يرتبط بالمجال المعلوماتي، ويترتب عليه إلحاق ضرر بالمجني عليه يقابله تحقيق منفعة للجاني. كما عرّفها الأستاذان Lestan وVivant بأنها طائفة من الأفعال المتصلة بالمعلوماتية والتي يمكن أن تستوجب العقاب وفقًا للقانون. أما الأستاذ Devéze، فقد أوضح أن الأمر لا يقتصر على مجرد إضفاء وصف قانوني على أفعال معينة، بل يتطلب بلورة مفهوم ذي طبيعة إجرامية يمكن إخضاعه للتكييف وفق القواعد المعمول بها في فروع القانون المختلفة، سواء المدني أو الجنائي أو المالي.

ذهب الفقيه الألماني Tiedemann إلى تعريف الجرائم المعلوماتية بأنها كل صور السلوك غير المشروع أو الضار بالمجتمع التي تُرتكب باستخدام الحاسب الآلي كوسيلة أساسية في التنفيذ.

يتبيّن من استعراض هذه الاتجاهات الفقهية أنها تتسم بقدر من العمومية والاتساع، الأمر الذي يصعّب حصرها في إطار جامع مانع، إذ إن كل تعريف ينطلق من زاوية تحليل مختلفة تبعًا للمنظور الذي يعتمده صاحبه، سواء كان تقنيًا أم قانونيًا أم وظيفيًا.

ومن أبرز التصورات الموسّعة في هذا السياق ما طرحه الفقيهان Miche وCerdo، حيث اعتبرا أن سوء استخدام الحاسب أو ما يُسمى بجريمة الحاسوب لا يقتصر على توظيفه كوسيلة لتنفيذ فعل مجرّم فحسب، بل يشمل كذلك حالات الدخول غير المصرح به إلى جهاز الغير أو إلى بياناته. كما يمتد المفهوم، في رأيهما، ليطال الاعتداءات المادية الواقعة على الحاسب ذاته أو على ملحقاته وتجهيزاته، فضلاً عن الاستخدام غير المشروع لبطاقات الائتمان، والعبث بأجهزة الصراف الآلي وما يرتبط بها من أنظمة تمويل إلكترونية، إضافة إلى تزييف المكونات المادية أو المعنوية للنظام المعلوماتي، بل وحتى سرقة الجهاز أو أحد أجزائه [14، ص45] .

وفي نطاق الفقه العربي برزت بدورها محاولات متعددة لصياغة مفهوم دقيق للجريمة المعلوماتية، تعكس اهتمام الباحثين بضبط هذا المصطلح في إطار قانوني منظم.

فقد ذهب اتجاه إلى تعريف الجريمة المعلوماتية بأنها كل فعل أو امتناع يتسم بالعمد، وينتج عن استعمال غير مشروع لتقنية المعلومات، ويستهدف الاعتداء على الأموال أو الحقوق ذات الطابع المعنوي. ويركّز هذا التعريف على عنصر القصد الجنائي وطبيعة الوسيلة التقنية المستخدمة، إضافة إلى محل الحماية القانونية.

ويرى اتجاه آخر أن الجريمة المعلوماتية تتمثل في كل سلوك إيجابي أو سلبي يترتب عليه إضرار بمكونات الحاسوب أو بشبكات الاتصال المرتبطة به، متى كان هذا السلوك مما يجرّمه قانون العقوبات ويقرر له جزاءً. ويبرز في هذا التصور الاهتمام بحماية البنية التقنية ذاتها باعتبارها محلًا للاعتداء.

المطلب الثاني

الحد من ارتفاع نسبة الجرائم عبر الذكاء الاصطناعي

تتباين طبيعة الجريمة المعلوماتية تبعًا للزاوية التي يُنظر من خلالها إلى محل الاعتداء المرتبط بالنظام المعلوماتي، قد يكون النظام المعلوماتي ذاته . بمكوناته المادية أو برامجه أو بياناته . هو محل الجريمة، عندما ينصب الفعل الإجرامي مباشرة على تخريبه أو تعطيله أو العبث بمحتواه. وفي هذه الحالة يكون الاعتداء واقعًا على الكيان التقني نفسه بوصفه موضوعًا للحماية القانونية. ومن جهة أخرى، قد لا يكون النظام المعلوماتي هو الهدف المباشر، بل يُستعمل كوسيلة أو أداة لتنفيذ جريمة أخرى، كأن يُستغل في الاحتيال أو التزوير أو الاستيلاء غير المشروع على الأموال:

أ . كون النظام المعلوماتي موضوعا للجريمة المعلوماتية.

في هذا الإطار يمكن التمييز بين صور الجرائم المعلوماتية بحسب طبيعة محل الاعتداء، ومدى اتفاقها مع أنماط الجرائم التقليدية المعروفة في القانون الجنائي.

فإذا انصبّ الفعل الإجرامي على المكونات المادية للنظام المعلوماتي، كالأجهزة والمعدات التقنية، فإن الأمر لا يخرج في جوهره عن كونه سرقة أو إتلافًا لهذه الوسائل، سواء تعلّق بالحاسب ذاته، أو الشاشات، أو شبكات الاتصال الخاصة، أو حتى الطابعات والملحقات المرتبطة به. وهنا يتقاطع الوصف القانوني مع الجرائم التقليدية التي تستهدف الأموال المادية الملموسة، أما إذا كان الاعتداء موجّهًا إلى العناصر غير المادية للنظام، كالبيانات والبرامج، فإن الصورة تختلف من حيث الطبيعة وإن اتفقت من حيث الأثر. ويشمل ذلك الاعتداء على البيانات المخزنة في ذاكرة الحاسب أو المتداولة عبر شبكات الاتصال، من خلال سرقتها أو نسخها أو إتلافها أو محوها أو تعطيلها. كما قد يمتد الفعل إلى برامج الحاسوب ذاتها عبر تزوير المخرجات الإلكترونية أو إفشاء محتواها، إضافة إلى ما يُعرف بسرقة وقت تشغيل الحاسب أو استغلال قدرته التشغيلية دون وجه حق، ومن ثمّ فإن التكييف القانوني يتحدد بحسب طبيعة محل الاعتداء.

ب . كون النظام المعلوماتي هو أداة الجريمة المعلوماتية ووسيلة تنفيذها.في هذه الصورة تحديدًا، لا يثور شك في أننا نكون أمام جرائم ذات طبيعة تقليدية من حيث التكييف القانوني، غير أن الوسيلة المستخدمة في تنفيذها تتمثل في النظام المعلوماتي أو جهاز الحاسب الآلي.

فالحاسب هنا لا يشكّل محل الاعتداء، وإنما يُستعمل كأداة لارتكاب الفعل المجرّم، بحيث يمكن للجاني توظيفه في ارتكاب جرائم كالسرقة أو الاحتيال أو خيانة الأمانة أو تزوير المحررات ذات الطابع المعلوماتي. ويتم ذلك من

خلال العبث بالبرامج أو البيانات أو آليات التشغيل داخل النظام، بما يؤدي إلى تحقيق النتيجة الإجرامية المرجوة، وعليه، فإن الاختلاف يكمن في وسيلة التنفيذ لا في جوهر الجريمة [15، ص47].

ترتبط الجريمة المعلوماتية ارتباطًا وثيقًا بالقطاع المصرفي والمالي، نظرًا لاعتماد هذا المجال بصورة متزايدة على النظم الرقمية في إدارة المعاملات وتداول القيم. وقد أفرزت الثورة المعلوماتية أدوات حديثة في نطاق التجارة والتعاملات، فلم يعد الإثبات مقصورًا على المستندات الورقية، بل ظهرت التسجيلات والمحررات الإلكترونية وسندات الشحن الرقمية، وأصبحت للمخرجات الإلكترونية حجية معتبرة إلى جانب الوثائق التقليدية.

ويعكس الواقع العملي اتجاهًا واضحًا نحو الاعتماد على الوسائل التقنية في الإثبات، مع بقاء وسائل الإثبات التقليدية قائمة، شريطة أن يتدخل المشرّع بتنظيم تشريعي يضبط حجيتها ويحدد شروط الاعتداد بها. وفي المقابل، فإن الجريمة المعلوماتية تشمل كل سلوك غير مشروع يتعلق بالدخول غير المصرح به إلى أنظمة المعالجة الآلية للبيانات أو التلاعب بها أو نقلها بغير حق. ومثل هذه الأفعال تكشف عن قصور كثير من النصوص الجنائية التقليدية في استيعاب المستجدات التقنية، الأمر الذي يستلزم تطويرًا تشريعيًا يواكب التحول الرقمي المتسارع، فإن حماية المعاملات الإلكترونية أصبحت ضرورة قانونية ملحّة.

يثار في هذا السياق تساؤل جوهري يتعلق بالمركز القانوني للمعلوميات وطبيعة الحماية التي يمكن أن تتمتع بها في إطار القواعد العامة.

فهل يعد الذكاء الاصطناعي قيمة قائمة بذاتها تستوجب الحماية لذاتها، أم أن قيمتها تنبع مما تمثله من مصالح وحقوق ومراكز قانونية ، والاعتداءً يستوجب المساءلة، شأنها في ذلك شأن سائر الأموال أو المصالح المحمية، ومن هنا تتحدد طبيعة الحماية القانونية المقررة[16، ص49].

كذلك استقر الرأي على أن الاستيلاء على معلومات الغير أو استغلالها دون سند مشروع يُشكّل خطأ يوجب المسؤولية، حتى وإن ثار الجدل حول طبيعتها القانونية. ولهذا سعى أنصار هذا الاتجاه إلى توفير حماية غير مباشرة للمعلومات من خلال دعوى المنافسة غير المشروعة، مستندين في ذلك إلى ما استقر عليه قضاء محكمة النقض الفرنسية في بعض أحكامها، ومن ثمّ حاول هذا الاتجاه إيجاد أساس قانوني بديل للحماية فقال القانون الفرنسي: "إن الغاية من دعوى المنافسة غير المشروعة هي تأمين حماية الشخص الذي لا يمكنه أن ينتفع بأي حق استئثائي". لذلك يذهب الأستاذ Debois بأن الملكية العلمية، ربما ستأتي يوما ويعترف بها لصاحب فكرة لم تحصل على حق براءة اختراع باعتبار أن الفكرة السابقة مستبعدة من مجال الملكية الذهنية.

استنادًا إلى هذا التصور، يُقال إن المعلوميات تكتسب قيمتها من واقعها الاقتصادي في السوق متى كانت قابلة للتداول وغير محظورة قانونًا، كما أنها ثمرة جهد ذهني لمن أنشأها، بما يجعلها منفصلة في قيمتها عن الدعامة المادية

التي تحملها. فهي ترتبط بمبدعها بعلاقة قانونية تشبه علاقة المالك بما يملكه، وتنشأ بينها وبينه رابطة تُشبه علاقة التبني، تُضفي عليها طابعًا شخصيًا واقتصاديًا في آنٍ واحد. ومن ثمّ يستند هذا الرأي إلى حجتين أساسيتين لمنحها وصف القيمة: الأولى تتمثل في بعدها الاقتصادي وقابليتها للتقييم المالي، والثانية في الصلة القانونية التي تربطها بصاحبها.

فإن هذا الاتجاه يمنح الذكاء الاصطناعي مكانة قانونية مستقلة، فلا توجد ملكية معنوية بدون الإقرار بالقيمة المعلوماتية، ولذلك فهو يرى القيمة المعلوماتية ليست بالشيء المستحدث إذ أنها موجودة من قبل في مجموعة ما [17، ص49].

المطلب الثالث

الذكاء الاصطناعي وتغير ادوات الجريمة

مهما بلغت درجة الصرامة والفعالية في إجراءات البحث والتحقيق المرتبطة بالإجرام المعلوماتي، فإن أثرها في الحد من إساءة استعمال التقنيات يظل نسبيًا ومحدودًا، ويعود ذلك إلى الطبيعة الخاصة للفضاء الرقمي، حيث تنتقل المعلومات بسرعة فائقة، وتُحدث الهجمات الإلكترونية . كالهجمات المعتمدة على الفيروسات والبرمجيات الخبيثة . أضرارًا جسيمة قد تمتد في لحظات إلى أنظمة ومواقع متعددة.

كما أن انخراط ذوي الخبرة التقنية في بعض هذه الجرائم يعقّد من مهمة الملاحقة والزجر، خاصة في بيئة الإنترنت التي تتسم بالتشعب وصعوبة التتبع، ومن ثمّ لا يكفي الاعتماد على الوسائل العقابية وحدها، بل يظل الخيار الأكثر فاعلية هو توظيف التقنية ذاتها كأداة دفاع، عبر تطوير أنظمة متقدمة لأمن المعلومات، وتحصين المواقع، وتأمين قواعد البيانات والشبكات باعتبارها خط الدفاع الأول في مواجهة المخاطر الرقمية، وبذلك تصبح الحماية التقنية ركيزة أساسية في التصدي لهذا النوع من الإجرام [18، ص38] .

ومن أبرز الوسائل التقنية المعتمدة لتعزيز أمن المعلومات ما يأتي:

1- كلمة السر: تُعد من أبسط أدوات الحماية وأكثرها شيوعًا،إذ تُستخدم لتقييد الولوج إلى الحاسوب الشخصي أو إلى ملفات محددة أو إلى النظام بأكمله، وتقتضي الحماية الفعالة عدم إفشاء كلمة المرور للغير، مع تثبيت برامج متخصصة لمكافحة الفيروسات، واتباع احتياطات الأمان عند الاتصال بشبكة الإنترنت، لاسيما التحقق من مصادر الرسائل الإلكترونية قبل فتحها.

Quarterly Refereed and Scientific Journal Issued By College of Law in Babylon University
Online ISSN:2075-7220 Print ISSN:2313-0377
https://iasj.rdd.edu.iq/journals/journal/view/153

2- التشفير: يُقصد به إعادة صياغة البيانات في صورة غير مفهومة بقصد إخفاء مضمونها الحقيقي، وذلك عبر تحويلها إلى رموز أو صيغ تقنية لا يمكن إدراك معناها إلا من قبل من يملك مفتاح فك التشفير، فهو وسيلة لحماية الوثائق والمستندات الإلكترونية من الاطلاع غير المشروع أو التجسس.

3- تلافي الأخطاء البشرية: إذ إن بعض المخاطر لا تعود إلى اختراق خارجي، بل إلى سلوك غير حذر من المستخدمين، مثل ترك الجهاز مفتوحًا دون رقابة، أو فتح مرفقات بريد إلكتروني مجهولة المصدر، أو اختيار كلمات مرور ضعيفة. وقد تؤدي مثل هذه التصرفات إلى نتائج خطيرة تمس أمن النظام المعلوماتي بأكمله.

ومن ثمّ فإن الجمع بين الوعي التقني والإجراءات الوقائية يشكّل أساس الحماية الفعالة [19، ص259] .

يُعد التفتيش في الإطار التقليدي إجراءً من إجراءات التحقيق لا يُباشَر إلا عند وقوع جناية أو جنحة، أو الاشتراك فيهما، مع توافر دلائل جدية تشير إلى وجود أشياء أو أدوات من شأنها كشف الحقيقة لدى المتهم أو لدى غيره، فالأصل أن التفتيش يرتبط بقيام جريمة محددة ووجود مبررات قوية تبرر المساس بحرمة الأماكن أو الخصوصية.

أما في المجال المعلوماتي، فإن الأمر يقتضي ابتداءً وجود جريمة معلوماتية منصوص عليها ضمن المنظومة الجنائية، وأن تكون قد وقعت بالفعل سواء أكانت جناية أم جنحة كما يشترط توجيه الاتهام إلى شخص أو أكثر بارتكابها أو المساهمة فيها، ويستلزم الأمر كذلك توافر دلائل قوية أو قرائن جدية تفيد باحتمال وجود أجهزة أو أنظمة معلوماتية يمكن أن تسهم في كشف الحقيقة، سواء لدى المتهم أو لدى غيره، أن "أمن المعلومات" يتجاوز كونه مجرد حماية تقنية للبيانات، ليعبر عن حالة من الطمأنينة المجتمعية إزاء سلامة البنى المعلوماتية من مختلف مصادر التهديد،فهو يُجسد ذلك الشعور الواقعي أو المتوقع بعدم تعرض مكونات المجتمع المعلوماتي، ولا سيما القطاعات الحساسة منه، لمخاطر طبيعية أو افتراضية، سواء كان منشؤها داخليًا أم خارجيًا. ويقتضي هذا المفهوم استعدادًا دائمًا، فرديًا ومؤسسيًا، لمواجهة أي اعتداء محتمل، عبر اعتماد تدابير تقنية وتنظيمية تكفل صون المعلومات من الجمع غير المشروع أو الاطلاع غير المصرح به، فضلًا عن سائر صور العبث أو الإخلال بسلامتها، وبذلك يغدو أمن المعلومات عنصرًا جوهريًا في حماية الاستقرار الرقمي للمجتمع. [20، ص325]

يتميّز الإجرام المعلوماتي بطبيعة تختلف عن الإجرام التقليدي الذي يقترن في الغالب باستخدام القوة أو العنف المادي. فمع أن بعض الجرائم المرتبطة بالأنظمة المعلوماتية قد تتقاطع مع الجرائم العادية من حيث النتائج أو الأهداف، فإن الوسيلة في هذا المجال تعتمد غالبًا على أساليب تقنية غير مباشرة.

فالمجرم المعلوماتي لا يحتاج إلى استعمال القوة الجسدية، بل يكفيه التلاعب بالبيانات أو البرامج داخل الحاسب ليقوم بمحوها أو تعطيلها. وقد يلجأ إلى زرع فيروسات أو استخدام ما يُعرف بالقنابل المنطقية أو الزمنية أو

برامج الديدان الإلكترونية، مما يؤدي إلى شلّ النظام المعلوماتي وإفقاده قدرته على أداء وظائفه المعتادة. وتكمن الخطورة في أن هذه الأفعال قد تُرتكب عن بُعد وبأدوات تقنية يصعب تتبعها.

وقد يتطور الأمر إلى مستوى الاحتراف، بحيث يتحول النشاط الإجرامي إلى ممارسة منظمة تهدد الأفراد والمؤسسات على حد سواء، وهو ما يضاعف من خطورته على المجتمع بأسره، ومن ثمّ فإن طبيعته التقنية تزيد من تعقيد مواجهته.

أ . الشباب الحديثي العهد بالتكنولوجيا المعلوماتية.

وهم الشباب الذين انبهروا بالثروة المعلوماتية وانتشار الحواسيب، ولذلك كان أولئك الشباب يرتكبون الجرائم المعلوماتية عن طريق استخدام الحواسب الخاصة بهم أو بمدارهم. وهذه الطبقة من الشباب لديها قدر لا بأس به من الخبرة المعلوماتية، ومن ثمة فهم يمارسون مواهبهم في استخدام الحاسوب بعرض اللهو أو هواية اللعب من أجل الوصول إلى نظم المعلوماتية سواء الخاصة بالوزارات الخاصة أو الشركات العملاقة أو الشركات التجارية أو المؤسسات المصرفية والبرامج العسكرية.... [21، ص89]. وقد يتطور الأمر بالنسبة لهذه الفئة من الشباب خاصة إذا كان بينهم من لديه علم ومعرفة بعملية البرمجة.

ورغم ما سبق فإن فئة من الشباب الذين ينخرطون في هذا المجال قد تكون دوافعهم في البداية مقتصرة على حب الاستطلاع أو التجربة أو التسلية التقنية، دون قصد مباشر لارتكاب جريمة معلوماتية. فهم أحيانًا يسعون إلى اختبار قدراتهم أو استكشاف الثغرات بدافع الفضول لا أكثر.

غير أن خطورة الأمر تكمن في احتمال انزلاق بعضهم تدريجيًا نحو ممارسات غير مشروعة، خاصة مع تنامي المهارات التقنية وغياب الوعي القانوني أو الرقابة الأخلاقية. فالفاصل بين الهواية والتعدي قد يكون دقيقًا، ومع تكرار السلوك قد يتحول الشخص من هاوٍ يعبث بدافع التجربة إلى محترف يتعمد استغلال مهاراته في ارتكاب أفعال مجرّمة.

ب . الأشخاص المحترفون ارتكاب الجريمة المعلوماتية.

تشير بعض الدراسات إلى أن الفئة التي تمتهن الجرائم المعلوماتية غالبًا ما تتراوح أعمارها بين الخامسة والعشرين والخامسة والأربعين عامًا، وهي مرحلة تجمع بين النضج المهني والقدرة التقنية، ويمكن التمييز في هذا السياق بين مرحلتين: الأولى تمثل بدايات الانخراط في عالم المعلوماتية، حيث يكون الشخص حديث العهد بالتقنيات والحواسيب، ويغلب على سلوكه طابع الهواية أو الفضول دون توجه إجرامي واضح. أما المرحلة الثانية فتتزامن مع ازدياد الخبرة واتساع انتشار الوسائل التقنية، حيث يبلغ التطور التكنولوجي مستوى متقدمًا يسمح بإدراك أعمق لآليات الأنظمة وإمكانات استغلالها.

وفي هذه المرحلة قد يتحول بعض الأفراد من مجرد هواة إلى محترفين في استغلال الثغرات التقنية وارتكاب أفعال غير مشروعة. وغالبًا ما تقع الجرائم المعلوماتية من أشخاص يعملون داخل مؤسسات أو أندية أو في إطار نظم معلوماتية رسمية، بحيث تكون لهم مسؤولية مباشرة عن تشغيل الأنظمة أو إدارتها. ومع معرفتهم الدقيقة بالتقنيات وأساليب التشغيل، يتمكنون من التلاعب بالأنظمة وتنفيذ أفعالهم دون إثارة الشبهات في البداية، ومن ثمّ فإن عامل الخبرة الداخلية يزيد من خطورة هذا النمط من الإجرام.

يتميّز الإجرام المعلوماتي عن الإجرام التقليدي بارتباطه الوثيق بتقنية المعلومات وبالتحولات التي أحدثتها ثورة المعلومات في بنية المجتمع المعاصر. فهذه الثورة لم تغيّر فقط وسائل الاتصال والتعامل، بل انعكست أيضًا على طبيعة الجريمة ذاتها، من حيث أدواتها وأساليبها وبيئتها. ومن ثمّ فإن أسباب انتشار هذا النوع من الإجرام تتأثر بصورة مباشرة بالتقدم التقني واتساع نطاق استخدام الأنظمة الرقمية.

وتكشف أنماط المجرمين المعلوماتيين عن تباين في الدوافع؛ فبعضهم يقدم على الفعل بدافع الهواية أو بدافع اللهو وإثبات القدرة التقنية، متأثرًا بالانبهار بإمكانات التكنولوجيا الحديثة. في حين يتجه آخرون إلى استغلال مهاراتهم لتحقيق مكاسب مالية سريعة، أو بدوافع شخصية كالرغبة في الانتقام أو إثبات الذات. وهكذا تتعدد البواعث بين ما هو تقني صرف وما هو مادي أو نفسي. [22، ص48]

وتكشف الواقعة كيف قد يتحول الانبهار التقني إلى سلوك منحرف إذا لم يُضبط بالوعي والمسؤولية [23، ص56] .

قد يكون الدافع المادي أحد أبرز المحركات نحو ارتكاب الجرائم المعلوماتية، إذ يسعى بعض الأفراد إلى تحقيق ثراء سريع من خلال تمكين الغير من الاطلاع على معلومات ذات طبيعة حساسة أو ذات قيمة خاصة لمن يطلبها. وللوصول إلى هذا الهدف، تُستخدم وسائل تقنية متعددة، الأمر الذي يجعل هذا الباعث من أكثر الأسباب إسهامًا في انتشار هذا النوع من الإجرام، خاصة عندما يقترن بضغوط مالية أو ديون متراكمة أو سلوكيات منحرفة كالإدمان، فيندفع الفاعل إلى استغلال خبرته التقنية لتحقيق مكاسب غير مشروعة، كما حدث في بعض الوقائع التي تورط فيها مبرمجون يعملون داخل مؤسسات، ومن ناحية أخرى، قد ترجع الدوافع إلى عوامل نفسية، كالشعور المبالغ فيه بالقدرة والسيطرة، حيث يعتقد البعض أن لهم الحق في تجاوز الأنظمة وإثبات تفوقهم عليها، فيتباهون بما يرتكبونه من أفعال غير مشروعة لإظهار مهاراتهم التقنية. وقد يكون الباعث أيضًا هو الانتقام، فيلجأ الفاعل إلى تخريب البرامج أو زرع فيروسات أو قنابل منطقية تُحدث أضرارًا جسيمة بالأنظمة المعلوماتية، وهكذا تتعدد الدوافع بين المادي والنفسي والشخصي [24، ص259] .

الخاتمة

بعد اتمام هذه الدراسة التي كانت بعنوان المسؤولية الجنائية عن جرائم الذكاء الاصطناعي والتي تناولت فيها ماهية المسؤولية الجنائية والذكاء الاصطناعي فضلا عن النصوص القانونية والاجراءات للمسؤولية الجنائية في الذكاء الاصطناعي وتوصل الباحث الى النتائج والتوصيات وكما يلي:

اولا : النتائج

1- ان الأحكام العامة للذكاء الاصطناعي لا تختلف عن الأحكام العامة للجريمة العادية التقليدية إلا فيما ندر في ركنها المادي وخاصة فيما يتعلق بعنصري المكان والزمان ، وما يتعلق بمدى انطباق القوانين الوطنية على بعض الأفعال التي ترتكب في الخارج وتحديد القضاء المختص داخل الدولة الواحدة .

2- أن السلوك الإجرامي قي هذه الجريمة عبارة عن تدفق للمعلومات عبر نظم الحاسب الآلي لا يمكن الإمساك ماديا بها

3- ينبغي الوقوف على تحليل سلوكها الإجرامي ، خاصة ما يتعلق ببعض الأفكار مثل فكرة المال في جريمة الاعتداء على المال الخاص أو المال العام ، وكذلك فكرة التزوير في مخرجات الحاسب الآلي.

4- يثير البحث في الطبيعة القانونية للجريمة المعلوماتية مسألة جوهرية تتعلق بالمركز القانوني لكل من البرامج والمعلومات داخل النظام القانوني، فالنقاش حول هذا الموضوع ينصب على تحديد ما إذا كانت البرامج والبيانات تُعد أموالًا بالمعنى القانوني، أم أنها تندرج ضمن الحقوق المعنوية التي تخضع لنظام قانوني خاص، كقواعد الملكية الفكرية. ويترتب على هذا التحديد بيان نطاق الحماية الجنائية المقررة لها، وما إذا كان الاعتداء عليها يُكيّف وفق الجرائم التقليدية، أم يستوجب نصوصًا خاصة تراعي طبيعتها التقنية، ومن ثمّ فإن تحديد الوضع القانوني للبرامج والمعلومات يُعد خطوة أساسية لفهم البنية القانونية للجريمة المعلوماتية وضبط حدود التجريم والعقاب في هذا المجال.

5- يثار التساؤل حول ما إذا كانت المعلومات تُعد قيمة قائمة بذاتها، أم أن قيمتها تندرج ضمن طائفة من القيم المستحدثة التي يمكن أن تكون محل اعتداء بوسائل متعددة، وقد انقسم الفقه في هذا الشأن إلى اتجاهين رئيسيين، يرى الاتجاه الأول، استنادًا إلى القواعد العامة في القانون الجنائي، أن محل السرقة يجب أن يكون شيئًا ماديًا قابلاً للحيازة والنقل، أي أن يتمتع بكيان ملموس يمكن الاستيلاء عليه بطريق الاختلاس، وهو ما يشكل الركن المادي للجريمة. وبناءً على ذلك، فإن المعلومات بحكم طبيعتها المعنوية وغير الملموسة ، لا تُعد من قبيل الأشياء التي تقبل الحيازة بالمعنى التقليدي، ولا تدخل في نطاق السرقة إلا في حدود ما تقرره قوانين الملكية الفكرية من حماية خاصة، وعلى ذلك تُستبعد المعلومات والأفكار المجردة من نطاق جريمة السرقة ما لم تكن مثبتة على دعامة مادية،

كقرص أو شريط أو وسيط تخزين مماثل. ففي هذه الحالة يكون الاعتداء منصبًا على الوسيط المادي ذاته، لا على المعلومة في ذاتها.

6- تثور إشكالية قانونية عند تكييف الفعل بوصفه سرقة لمال معلوماتي، إذ لا يطرح الأمر صعوبة كبيرة متى كان الاعتداء منصبًا على دعامة مادية تحتوي البيانات، كجهاز أو وسيط تخزين، حيث يمكن إخضاعه للقواعد التقليدية في جريمة السرقة، غير أن الإشكال الحقيقي يظهر عندما يتعلق الأمر بسرقة مال معلوماتي غير مادي، أي البيانات أو المعلومات في ذاتها، دون المساس بالدعامة التي تحملها، فهنا ينقسم الرأي حول ما إذا كانت المعلومات تُعد مالًا قابلاً للاستحواذ بذاته، أم أنها تظل مجرد قيمة معنوية لا تدخل ضمن المفهوم التقليدي للمال. ويذهب اتجاه إلى اعتبارها طائفة مستحدثة من القيم يمكن الاستيلاء عليها بصورة مستقلة عن الوسيط المادي، بما يبرر منحها حماية جنائية مباشرة.

ثانيا: التوصيات

1- ينبغي العمل على تطوير إطار تشريعي واضح ينظم استخدام تقنيات الذكاء الاصطناعي في المجال الجنائي، بحيث يحدّد حدود الاستخدام، ويضمن احترام الحقوق والحريات الأساسية، ولا سيما مبدأي الشرعية والخصوصية. فغياب التشريع الدقيق قد يفتح المجال أمام ممارسات تعسفية أو استخدامات غير منضبطة للتقنيات الحديثة.

2- توصي الدراسة بضرورة تعزيز مبدأ الشفافية في الأنظمة الذكية المستخدمة في العدالة الجنائية، من خلال اعتماد خوارزميات قابلة للتفسير والمراجعة، بما يمكّن القضاة والمحامين من فهم آليات اتخاذ القرار، ويمنع الانحيازات الخفية التي قد تؤثر في العدالة.

3- الاستثمار في بناء القدرات البشرية داخل المؤسسات العدلية، عبر تدريب القضاة وأعضاء الادعاء العام وأجهزة إنفاذ القانون على فهم أدوات الذكاء الاصطناعي واستخدامها بشكل فعّال ومسؤول. فنجاح هذه التقنيات لا يعتمد على توفرها فقط، بل على كفاءة من يديرها ويوظفها.

4- ضرورة اعتماد مقاربة متوازنة تجمع بين الكفاءة التقنية والعدالة الاجتماعية، بحيث لا يؤدي استخدام الذكاء الاصطناعي إلى تكريس التمييز أو الإقصاء، خصوصاً تجاه الفئات الهشة. ولهذا، يجب إخضاع الأنظمة الذكية لاختبارات دورية للكشف عن أي تحيزات محتملة ومعالجتها.

5- تعزيز التعاون الدولي وتبادل الخبرات بين الدول في مجال استخدام الذكاء الاصطناعي في السياسة الجنائية، للاستفادة من التجارب المقارنة وتبنّي أفضل الممارسات، بما ينسجم مع الخصوصيات القانونية لكل دولة.

المصادر

[1] سعد غالب ياسين، نظم المعلومات الإدارية وتكنولوجيا المعلومات، دار المناهج، عمان، الطبعة الأولى، 2006.

[2]منال محمد الكردي، الذكاء الاصطناعي ، دار العلم، لبنان، 1998.

[3]منال محمد الكردي، الذكاء الاصطناعي ، دار العلم، لبنان، 1998.

[4] ابراهيم العيسوي ، التنمية : المفهوم والمؤشرات مذكرات تدريبية غير منشورة ، المعهد العربي للتخطيط ، الكويت ،1994.

[5] جميل طاهر، النفط والتنمية المستديمة في الاقطار العربية الفرص والتحديات ، المعهد العربي للتخطيط ، الكويت،1997 .

[6] انمار امين حاجي، بسام يونس إبراهيم ، عادل موسى يونس ، الاقتصاد القياسي ، ط1 ، دار عزة للنشر والتوزيع ، الخرطوم ، السودان، 2002.

[7] عبد الله الكندلي ، البيئة والتنمية المستدامة ،مكتبة المهند ، الكويت ، 1992.

[8] ف. دوجلاس موسيشيت ، مبادئ التنمية المستدامة ، ترجمة بهاء الدين شاهين ، الدار الدولية للاستثمارات الثقافية ، القاهرة ، مصر ،2000.

[9] د. جمال ابراهيم الحيدري ، احكام المسؤولية الجزائية ،منشورات زين الحقوقية ، ط1، 2010.

[10] وليد اسماعيل السيفو ،المدخل الى الاقتصاد القياسي ،مديرية دار الكتب للطباعة والنشر ، جامعة الموصل ، الموصل ، العراق ،1988.

[11] "محمد أحمد أمين الشوابكة : "الجريمة المعلوماتية". دار الثقافة، عمان، طبعة 2004."

[12] "محمد علي العريان: "الجرائم المعلوماتية". دار الجامعة الجديدة للنشر. طبعة 2004."

[13] "محمد سامي الشوا: "ثورة المعلومات وانعكاساتها على قانون العقوبات". دار النهضة العربية، القاهرة. 1994."

[14] محمد علي العريان ، الجرائم المعلوماتية". دار الجامعة الجديدة للنشر. طبعة 2004..

[15] محمد علي العريان: الجرائم المعلوماتية". دار الجامعة الجديدة للنشر. طبعة 2004..

[16] محمد علي العريان: الجرائم المعلوماتية". دار الجامعة الجديدة للنشر. طبعة 2004..

[17] محمد علي العريان: الجرائم المعلوماتية". دار الجامعة الجديدة للنشر. طبعة 2004..

[18] "أحمد آيت الطالب :مقال: قضايا عامة، نبض المجتمع. مجلة الشرطة. العدد 3 أبريل 2005."

[19] "إيمان فاضل السامرائي، هيثم محمد الزغبي: "نظم المعلومات الإدارية". الطبعة الأولى، دار صفاء للنشر والتوزيع. عمان. 2005."

[20] "علي بن ضيبان الرشيدي:مقال: "التقنية والأمن". مجلة كلية الملك خالد العسكرية، العدد 81 بتاريخ 2005/06/01. "

[21]ضياء عبد الله الاسدي وعلي سعد عمران ، المسؤولية الجزائية لعضو المجلس النيابي ، مكتبة زين الحقوقية والادبية بيروت ، 2013.

[22]محمد أحمد أمين الشوابكة : "الجريمة المعلوماتية". دار الثقافة، عمان، طبعة 2004.

[23] د. عمار عباس الحسيني ، مبدأ شخصية العقوبة ودوره في تحقيق العدالة الجنائية ، بحث منشور في مجلة الكلية الإسلامية الجامعة ، العدد السادس ، 2009.

[24] إيمان فاضل السامرائي، هيثم محمد الزغبي: "نظم المعلومات الإدارية". الطبعة الأولى، دار صفاء للنشر والتوزيع. عمان. 2005.