Naif Arab University for Security Sciences
Arab Journal for Security Studies
المجلة العربية للدراسات الأمنية
https://journals.nauss.edu.sa/index.php/ajss
AJSS

Artificial Intelligence Applications in the Egyptian Litigation System: Prospects and Challenges

تطبيقات الذكاء الاصطناعي في منظومة التقاضي المصرية: آفاق وتحديات

مصطفى علي العقبي
وزارة الداخلية المصرية، جمهورية مصر العربية

Mostafa Ali Elokaby
Egyptian Ministry of Interior, Arab Republic of Egypt

Received on 24 Sept. 2024; accepted on 25 Feb. 2025; available online on 24 June 2025

Abstract

Recently, Egypt has been enhancing its cybersecurity legislation to counter the increasing digital threats. This includes the enactment of the Personal Data Protection Law and the Information Technology Crimes Law, reflecting Egypt's commitment to combating cybercrime and generally protecting data.

This study delves into the influence of these legal advancements on the judicial system, covering multiple facets. Cybersecurity laws establish a legal framework for punishing those responsible for cybercrimes and bolster capabilities in investigating and collecting digital evidence. Furthermore, the new legislation facilitates effective security measures for safeguarding sensitive data.

This study has reached several conclusions, including that digital transformation in the judicial and security systems has become inevitable. It is now essential for the Egyptian legislator to keep pace with this development. Furthermore, the substantive and procedural legislative framework is not aligned with the advancements in the judicial system and conflicts with established legal principles, such as the principle of public hearings.

We also reached several recommendations, including the necessity for the legislator to intervene by enacting a special law on artificial intelligence that includes modern

Keywords: *security studies, cybersecurity laws, judicial system, artificial intelligence, digital transformation, data protection, cybercrimes*

المستخلص

بدأت مصر في الآونة الأخيرة في تعزيز تشريعات الأمن السيبراني لمواجهة التهديدات الرقميَّة المتزايدة، ومن بين هذا التطور إصدار قانون حماية البيانات الشخصيَّة، وقانون مكافحة جرائم تقنية المعلومات، وهو ما يعكس التزام الدولة المصريَّة بمكافحة الجرائم السيبرانيَّة وحماية البيانات عامة.

ونتناول في هذا البحث أثر هذه التطورات على منظومة التقاضي في عدة جوانب؛ حيث توفر قوانين الأمن السيبراني إطارًا قانونيًّا لمعاقبة المتسببين في الجرائم السيبرانيَّة، كما تعزِّز القدرة على التحقيق وجمع الأدلة الرقمية، كما تتيح التشريعات الحديثة تدابير أمنية فعَّالة لحماية البيانات الحساسة.

وانتهت هذه الدراسة إلى عدة نتائج منها: أن التحول الرقمي في المنظومة القضائية والأمنية أصبح يفرض نفسه بشكل لا مفر منه، على نحو يُلزم بمواكبة هذه الثورة التكنولوجية، كما انتهينا إلى عدم مواكبة المنظومة التشريعية الإجرائية والموضوعية، للتطور الحالي في منظومة القضاء، بالإضافة للتعارض مع الأسس القانونية الراسخة كمبدأ علانية الجلسات.

كما وصلنا إلى عدة توصيات منها: ضرورة تدخل المشرع بإصدار قانون خاص بالذكاء الاصطناعي، يتضمن قواعد موضوعية وإجرائية

الكلمات المفتاحية: الدراسات الأمنية، قوانين الأمن السيبراني، النظام القضائي، الذكاء الاصطناعي، التحول الرقمي، حماية البيانات، الجرائم الإلكترونية

* Corresponding Author: *Mostafa Ali Elokaby*
Email: mostafa.okaby@gmail.com

doi: 10.26735/UKME7622

Production and hosting by NAUSS

1319-1241© 2025. AJSS. This is an open access article, distributed under the terms of the Creative Commons, Attribution-NonCommercial License.

حديثة تتناسب مع الطبيعة الاستثنائية للتحديات المتوقعة من استخدام هذا النوع من التكنولوجيا، وكذلك ضرورة تعزيز التعاون الدولي الأمني والقضائي في مجال الأمن السيبراني؛ نظرًا للطبيعة العابرة للحدود لهذه الجرائم.

substantive and procedural rules to address the exceptional nature of the challenges posed using this technology. Additionally, there is a need to strengthen international security and judicial cooperation in the field of cybersecurity due to the exceptional nature of these cross-border crimes.

1. المقدمة

في إطار مواكبة التحول الرقمي الحالي، واستخدام تطبيقات الذكاء الاصطناعي في كافة المجالات، اتجهت الدولة المصريَّة إلى رقمنة النظام القضائي وإجراءاته اتفاقًا مع رؤية مصر 2030، ووفقًا لما أكدته الإستراتيجية الوطنية لحقوق الإنسان التي أطلقها الرئيس المصري في سبتمبر 2021، سعيًا وراء تطوير منظومة التقاضي وتيسيرًا على المتقاضين.

وفي هذا الإطار تبنت وزارة العدل المصريَّة إستراتيجيَّة تواكب الثورة التكنولوجية التي من المؤكد أنها ستمتد إلى منظومة القضاء في جميع الجوانب، وتهدف تلك الإستراتيجية بالتعاون مع وزارة الاتصالات وكافة الجهات المعنية لتقديم الدعم اللوجيستي للتوجه نحو التحول الرقمي في كافة قطاعات الوزارة، وكانت البداية بقطاع الشهر العقاري وإصدار التوكيلات وغيرها من الخدمات، وكذلك منظومة التقاضي الإلكتروني في المحاكم الاقتصادية.

وتتضمن تلك الإستراتيجية محورين أساسيين، المحور الأول: تطور وأتمتة الأنظمة القائمة بالفعل وإعادة هيكلتها وتحقيق الاندماج مع الجهات الحكومية الأخرى المعنية، والمحور الثاني: هو إجراء جلسات المحاكمات عن بعد مع توفير كافة الضمانات والإمكانات الفنية لتحقيق الوصول عن بعد لكافة عناصر المنظومة القضائية للمحكمة من متقاضين ومحامين وشهود، كما تتضمن هذه الخطة ربط درجات المحاكم المختلفة والنيابات المختلفة والمكتب الفني للنائب العام بالتعاون مع الأمانة العامة لوزارة الداخلية والمحاكم المختلفة على مستوى الجمهورية (Abou-eleid, 2020).

ولم تكن النيابة العامة بعيدةً عن مواكبة مسار التطور التكنولوجي، فقامت مؤخرًا في ضوء إستراتيجيتها العامة في التحول الرقمي وتيسير سبل تقديم الخدمات الرقمية إلى المتعاملين معها عبر بوابتها الإلكترونية، بإطلاق المرحلة الأولى من «خدمات النيابة الجنائية»، حيث تقدم النيابة العامة من خلال بوابتها الإلكترونية خدمات الحصول على بعض الأوراق الرسمية، كالشهادات وصور محاضر الشرطة وتحقيقات النيابة العامة والأحكام القضائية ومحاضر الجلسات، بأن يتقدم ذوو الشأن من المحامين بطلبه ويسدد الرسوم من خلال تلك البوابة، ومن ثم يتسلم الورقة الرسمية المطلوبة بمقر مكتبه الخاص، على أن تكون تلك المرحلة تجريبية، تجري بنيابات محافظة الإسماعيلية تمهيدًا لتشغيلها تباعًا بكافة المحافظات.

فضلًا عن تطور الربط الرقمي بين النيابة العامة وأقسام الشرطة فيما يتعلق بقيد المحاضر بكافة أنواعها، وأتمتة قرارات النيابة العامة ومتابعة تنفيذها، عن طريق منظومة الربط الإلكتروني التي استحدثت في إطار إستراتيجية التحول الرقمي بين وزارة الداخلية ووزارة العدل والسلطات القضائية المختلفة.

ولكن في الحقيقة فإن التحول الرقمي يفتح الباب أمام عدة إشكاليات في الواقع العملي وتحديات يفرضها التعامل القضائي في الفضاء السيبراني، تبرز أهم هذه التحديات في حماية المنظومة القضائية الرقمية من مخاطر الهجوم السيبراني، فضلًا عن المشكلات المتعلقة بالخصوصية وحماية البيانات الشخصية، وحقوق الإنسان والتمييز والتحيز الخوارزمي لتطبيقات الذكاء الاصطناعي، بالإضافة للمشكلات المتعلقة بإمكانية الوصول إلى المنظومة القضائية الرقمية والعقبات الفنية والاقتصادية التي تعرقل التقدم نحو دخول هذه الإستراتيجية حيز التنفيذ.

أهمية البحث

- بيان أهمية تشريعات الأمن السيبراني في مصر كمسألة حيوية، في ظل التهديدات المتوقعة والمتزايدة من التطور التكنولوجي السريع.
- دراسة الآثار المتوقعة لقوانين الأمن السيبراني في منظومة التقاضي، وما تقدمه من فرص وما تواجهه من تحديات.
- بيان التحديات التشريعية والتقنية التي تواجه منظومة التحول الرقمي القضائي في مصر.
- استعراض تطور سياسة المشرع المصري لمواكبة التطور التكنولوجي، ومواجهة مخاطر أمن المعلومات والبيانات.

أهداف البحث

- بيان مدى تكامل القوانين السيبرانيَّة في مصر، وبيان أوجه القصور فيها.
- تقييم مدى فاعلية سياسة المشرع المصري الحالية في مواكبة التطور التكنولوجي.

- بيان أثر تطور قوانين الأمن السيبراني على منظومة التقاضي، والفرص والتحديات المحتملة.
- بيان المقصود بالتقاضي الرقمي وإجراءاته، وماهية المحاكمة الافتراضية.

مشكلة البحث

- **المشكلة الرئيسة**

في ظل التطورات المتسارعة في مجال تكنولوجيا المعلومات واستخدام الذكاء الاصطناعي في منظومة القضاء، برزت الحاجة إلى تطوير البنية التشريعية لضمان فاعليَّة هذا التحول وحماية حقوق المتقاضين، وتتمثل المشكلة الرئيسة لهذا البحث في مدى قدرة التشريعات الوطنية، ولا سيما قانون الإجراءات الجنائية، على مواكبة متطلبات الأمن السيبراني، وتأمين بيئة التقاضي الإلكتروني في مواجهة التهديدات التقنية والقانونية الجديدة.

- **المشكلات الفرعية**

وينتج عن المشكلة الرئيسة لهذه الدراسة مجموعة من المشكلات الفرعية أبرزها:

- عدم مواكبة التشريعات الموجودة حاليًّا للتطور العالمي في مجال الأمن السيبراني، يُعدُّ من أهم التحديات التي تواجه التطور التكنولوجي في منظومة القضاء، خاصة فيما يتعلق بقانون الإجراءات الجنائية.
- العقبات المالية والتقنية والكفاءات البشرية التي يمكنها استخدام المنظومة الرقمية الجديدة.
- مخاطر الأمن السيبراني والهجوم الإلكتروني المحتمل على المنصات والمواقع الإلكترونية لمنظومة التقاضي.
- مشكلات الاختصاص القضائي في مواجهة الجرائم السيبرانيَّة خاصة مع كونها جرائم عابرة للوطنية.
- المشكلات المتعلقة بالخصوصية وحماية البيانات الشخصية وحماية حقوق الإنسان، والحاجة إلى سد الفجوة بين هذه المبادئ وغاية تحقيق الأمن.
- المشكلات المتعلقة بحماية الدليل الرقمي، خاصة في ظل أساليب التزييف والتحايل الإلكتروني.

منهج البحث

تم اعتماد المنهج الوصفي التحليلي لبيان أثر تطور قوانين الأمن السيبراني على منظومة التقاضي، والفرص والتحديات التي قد يواجهها هذا التطور، وطرق مواجهة هذه التحديات، كما نوضح ماهية الذكاء الاصطناعي والأمن السيبراني ومفهوم المحكمة الإلكترونية والمحكمة الافتراضية، وصولًا إلى غاية تحقيق التطور الذي أصبح واقعًا لا مفر منه في منظومة التقاضي مع تحقيق الضمانات الكاملة لعناصر المنظومة القضائية وحمايتها من الأخطار السيبرانيَّة المتوقعة.

2. المبحث الأول: ماهية الذكاء الاصطناعي والمحاكم الإلكترونية

أصبح الذكاء الاصطناعي أحد أبرز التطورات التي من المتوقع أن تشكل الحياة المستقبلية في عصر تزايدز فيه وتيرة التطور التكنولوجي، وتجاوزت قدرات الذكاء الاصطناعي حدود الكيانات الصناعية والعلمية، وامتد تأثيره إلى منظومة القضاء، ممهدًا الطريق أمام مفهوم جديد للعدالة، إذ يتميز بقدرات هائلة على معالجة وتحليل كميات هائلة من المعلومات بسرعة ودقة تفوق القدرات البشرية.

وتعدُّ المحاكم الإلكترونية قفزة في إدارة القضايا والتعاملات القضائية الرقمية عامة؛ إذ تُعدُّ حلًا مبتكرًا لتحسين العملية القضائية يجمع بين الذكاء الاصطناعي والأنظمة الإلكترونية وتقديم خدمات قانونية بطريقة أكثر فاعلية وشفافية.

2. 1. المطلب الأول: مفهوم الذكاء الاصطناعي

ونتناول في هذا المبحث المقصود بالذكاء الاصطناعي والدور الذي يؤديه في المجال الأمني، وفي المنظومة القضائية على النحو التالي:

2. 1. 1. الفرع الأول: تعريف الذكاء الاصطناعي

يُعرَّف الذكاء الاصطناعي (Artificial Intelligence - AI) بأنه استخدام تقنيات وخوارزميات محددة بهدف تنفيذ مهمة محددة، أو أداء عمل محدد، ويتم برمجة الجهاز الذكي بشكل يسمح له بتلقي المدخلات بشكل تلقائي، ومن ثم تنفيذ الإجراءات المطلوبة وفقًا للبرنامج المحدد، ويمكن للذكاء الاصطناعي أن يتعلم ويتكيف من خلال تحليل البيانات واكتساب المعرفة الجديدة (Boden, 2018, p.5).

كما يعرف بأنه أحد فروع علوم الحاسوب، ويُعدُّ عنصرًا مهمًّا في صناعة التكنولوجيا الرقمية خلال عصر الثورة الصناعية الرابعة. ويتميز الذكاء الاصطناعي بقدرة الأجهزة الرقمية والحواسيب على أداء مهام تحتاج إلى ذكاء يُشبه الذكاء البشري، كالقدرة على التفكير والاستفادة من الأخطاء المرتكبة، وغير ذلك من المهام التي تتطلب قدرات ذهنية. وعامة يهدف علم الذكاء الاصطناعي إلى فهم طبيعة القدرات البشرية من خلال تطوير برمجيات وأنظمة حاسوبية قادرة على محاكاة الأداء الذكي للإنسان (خوالد، 2019، ص. 9).

وتقوم هذه التكنولوجيا على عددٍ من الخوارزميات الرياضية المنطقية المتسلسلة لحل مشكلة ما متجاوزة القدرات الطبيعية للبشر (عبد الكريم، 2022، ص. 910)، وتستمر الجهود في سبيل تحقيق التقدم في مجال تطوير الذكاء الاصطناعي الذي يعمل بشكل مستقل دون الحاجة إلى إشراف بشري، بحيث يكون قادرًا على استخدام خوارزميات التعلم الآلي المتطورة لتجاوز القدرات البشرية، وفي هذا الإطار كان السعي في النماذج الأولية لهذه الخوارزميات في اتجاه تقليد الوظائف والسلوكيات البشرية بشكل دقيق جدًا (Osoba, Welser IV, 2017, p.5).

2. 1. 2. الفرع الثاني: الذكاء الاصطناعي في المنظومة القضائية والأمنية

في منظومة العدالة الرقمية، يمكن تعريف هذه التكنولوجيا بأنها عبارة عن برمجيات حسابية تحلل مجموعة ضخمة من البيانات القضائية، سواء أكانت أحكامًا أو سوابق قضائية، تهدف هذه البرمجيات إلى استنتاج الأسباب والنتائج الكامنة وراء هذه الأحكام والقرارات، وكذلك التحقق من مدى ملاءمة مقدار التعويض في الأحكام التي صدرت بالتعويض. وهذا النهج التكنولوجي يُستخدم كوسيلة لتقليل نسبة الأخطاء في الأحكام والقرارات الصادرة عن العدالة التقليدية، ويُعدُّ خطوة مساعدة للقضاء في الوصول إلى حكم وقرار قضائي أكثر عدالة وإنصافًا (Amankwaa, McCartney, 2018).

كما يمكن استخدم تطبيقات الذكاء الاصطناعي في كتابة القضايا وترتيبها والترجمة القانونية والتأكد من صحة التسجيلات المرئية والمسموعة، فضلًا عن كشف التزوير في المحررات والأدلة الرقمية، واستخدام الذكاء الاصطناعي في تزكية الشهود (الجلعود، 2023، ص.47)، ومن المتوقع أن تتجه المنظومة القضائية المصريَّة قريبًا إلى الاستفادة من هذه الاستخدامات لتعزيز سير العملية القضائية وتحسين جودتها وتعزيز مبادئ العدالة الناجزة.

كما تؤدي تقنيات الذكاء الاصطناعي دورًا كبيرًا في التنبؤ بالجريمة والوقاية منها، وكذلك في الكشف عن المجرمين ومكافحة الجريمة، ويُعزى استخدام هذه التقنيات إلى الحاجة إلى تعزيز قدرات البحث الجنائي بفضل سرعتها ودقتها في كشف الجرائم، وتقديم أدلة قوية للقضاء، وفي مجال العمل الأمني أحدث الذكاء الاصطناعي تغييرات جذرية، سواء في التنبؤ بالجرائم قبل حدوثها أو في التحري عند وقوعها، وهو ما أثار جدلًا حول فوائدها ومخاطرها، وتحدياتها الأمنية، وشرعيتها، مع ما تفرضه الحاجة إلى تشريعات أكثر ملاءمة لمواجهة تحديات الذكاء الاصطناعي، ومن أمثلة تطبيقاته: قراءة لوحات السيارات، التنبؤ الآلي بالجرائم، الشرطي الآلي، التعرف على الوجوه في الأماكن العامة (علاوي، عبد المجيد، 2023، ص. 372) و(خليفة، 2018، ص. 32).

ومما لا شك فيه أن الاتجاه إلى استخدام تطبيقات الذكاء الاصطناعي والتكنولوجيا المتطورة عامة في المنظومة القضائية يتطلب تعديل وتطوير الهياكل الإدارية والتنظيمية داخل المحاكم المختلفة، وعالميًّا تباينت الرؤى التنفيذية والتشريعية حول تنفيذ الاتجاهات التقنية الحديثة في مجال القضاء تبعًا لثقافة كل دولة وإمكاناتها الاقتصادية، إلا أن هذه الرؤى ما زالت تحديات كبيرة أمام الباحثين ورجال القضاء وصولًا لصيغة منضبطة آمنة على نحو يضمن تحقيق العدالة دون إخلال بالضمانات التي كفلها الدستور والقانون (Pro-copiuck, 2018, p.492).

وعلى المستوى القضائي، بدأت وزارة العدل المصريَّة في الأخذ ببعض أدوات التطور التكنولوجي في المحاكم المختلفة، فعلى سبيل المثال لا الحصر، كتابة المحاضر والقرارات والتحقيقات إلكترونيًّا في بعض النيابات، بالإضافة للاستعانة بتقنية الفيديو كونفرانس في تجديد الحبس الاحتياطي، فيما يعرف بـ "تجديد الحبس الاحتياطي عن بعد" (علي، 2021، ص. 6).

2. 2. المطلب الثاني: ماهية المحاكم الإلكترونية

لا تعدُّ المحاكم الإلكترونية كما يتخيل البعض عبارة عن جهاز قضائي خالٍ من وجود القضاة، أو محكمة تحكم النزاعات بصورة آلية بواسطة خوارزميات كمبيوتر مدمجة، أو عبر تدخل مسؤول عن إدارتها إلكترونيًّا، بل هي بنية تحتيَّة قضائيَّة تسعى لمعالجة الدعاوى والمنازعات بكافة أنواعها، ومن ثمَّ تمكين المواطنين من تقديم الأدلة والمستندات والدفوع بطريقة إلكترونية ذات تكلفة مقبولة، وفق آليات تضمن إعلان الخصوم بتفاصيل الدعوى بمجرد قيدها إلكترونيًّا، على أن تتوافر للمحاكم البنية التحتية والعناصر الفنية المدربة لإصدار قرارها العادل في أسرع وقت ممكن إلكترونيًّا مع توفير كافة الضمانات المتعلقة بالمحاكمات (Gerry, Muraszkiewicz & Iannelli, 2018, p.913).

إلا أننا لا يمكن أن نغفل المخاوف التي تحيط بالاندماج داخل منظومة القضاء الرقمي في المحاكم الإلكترونية، وخصوصًا فيما يتعلق بالقواعد الأساسية للعملية القانونية، ومع ما هو متوقع من أن تصبح منظومة التقاضي الإلكتروني هي أساس العملية القضائية وانتهاء منظومة القضاء التقليدي (محمود، 2020، ص. 28)، وتحديدًا فيما يتعلق بضمانات المتهم في مرحلة المحاكمة ومبدأ علنية الجلسات، وتمثيل الخصوم والحق في الاستعانة بمحامٍ.

ونتناول في هذا المطلب المقصود بالمحكمة الإلكترونية والغاية وراء استحداث هذا النوع من المحاكم، كما نستعرض مصطلح المحاكم الرقمية والمحاكم الافتراضية والفرق بينها وبين المحاكم الإلكترونية على النحو التالي:

2. 2. 1. الفرع الأول: تعريف المحكمة الإلكترونية والهدف منها

تُمثل المحاكم الإلكترونية واحدة من تطبيقات ثورة المعلومات وتكنولوجيا الاتصالات، وتُجسد فكرة «التقاضي الإلكتروني» أو «التقاضي عن بعد»، واتجهت العديد من الدول نحو هذا النهج؛ حيث يُمكن من خلال التقاضي الإلكتروني عمل الإجراءات القضائية والمحاكمات في بيئة رقمية بدلًا من البيئة التقليدية وجهًا لوجه. (Ward, 2015, p 341-358)

وتعددت التعريفات الفقهيَّة لمصطلح المحكمة الإلكترونية رغم خلو معظم التشريعات الإجرائية من بيان واضح لمفهوم التقاضي الإلكتروني، وتدور هذه التعريفات حول أنها عبارة عن نموذج حديث للمحاكم، يعتمد على الربط الشبكي عبر الإنترنت لتمكين الفصل في النزاعات المعروضة أمامها، تستخدم هذه المحاكم تقنيات عالية الحداثة وأنظمة إلكترونية متطورة لتسريع عملية الفصل في الخصومات؛ مما يوفر سهولة ويسرًا للمتقاضين (منديل، 2014، ص. 104)، إذ تمكنهم من إرسال وقبول المستندات بشكل إلكتروني وفق منظومة إلكترونية تربط بين المتقاضين والمحامين والمحكمة.

الهدف من المحاكم الإلكترونية

تُعدُّ الغاية من المحاكم الإلكترونية هي تحسين جودة وفاعلية منظومة التقاضي، ومن ثم تحقيق دقة القرارات المتوقع صدورها في القضايا المنظورة أمامها، وتحقيق العدالة الناجزة عن طريق إجراءات جنائية محسنة ومستحدثة تتجاوز حدود الإجراءات النمطية المتبعة أمام القضاء التقليدي؛ إذ تتيح تطبيقات الذكاء الاصطناعي للقضاة تفنيد القضايا المنظورة أمامهم وتحديد الأولويات، وترتيب القضايا من حيث أهمية اتخاذ قرار قضائي سريع حمايةً للحقوق والمراكز القانونية المستقرة للمتقاضين، دون الحاجة للانتقال بشكل مستمر إلى المحكمة لمتابعة جلسات القضية.

كما أن المحاكم الإلكترونية تعمل وفق منظومة خوارزمية معززة، تمكن النظام عند استقبال أوراق القضايا من الخصوم من القيام بتحديد المحاكم التي تختص بنظر هذا النوع من القضايا ابتداءً قبل السير في إجراءات التقاضي، وهو ما يغلق الباب أمام الدفوع الشكلية المتعلقة بالاختصاص الولائي والمكاني للمحكمة التي يتم نظر الدعوى أمامها، وهو ما كان من شأنه تعطيل سير العملية القضائية، وإطالة أمد الخصومة وفقًا للقضاء التقليدي؛ إذ يُعدُّ بذلك هذا النوع من المحاكم أحد أهم أدوات تحقيق العدالة الناجزة التي كانت وما زالت هدفًا للمشرع الجنائي المصري، لكن مع استمرار الحق في إثارة الدفوع الموضوعية أو الدفع بعد القبول في أي حالة كانت عليها الدعوى.

ومواكبةً لهذا التطور أعلنت محكمة استئناف القاهرة عن إطلاق خدمة الاستعلام الإلكتروني عن مواعيد الجلسات من خلال الموقع الإلكتروني لبوابة الحكومة المصريَّة، كما صدر القانون رقم 164 لسنة 2019 بشأن تعديل بعض أحكام قانون إنشاء المحكمة الاقتصادية رقم 120 لسنة 2008. وقد تضمنت التعديلات الجديدة استحداث المواد من 15 إلى 22، التي تنظم قواعد التقاضي الإلكتروني أمام المحاكم الاقتصادية، بحيث يتم الآن تقديم الدعاوى والطعون في الأحكام إلكترونيًّا، وإعلان الخصوم بطرق إلكترونية، وإرسال الملفات والمذكرات وطلبات الدعاوى من خلال الموقع الإلكتروني المعدّ لذلك.

2. 2. 2. الفرع الثاني: المحاكم الرقمية والمحاكم الافتراضية

المحاكم الرقمية

ظهر مؤخرًا في المنظومة القضائية مصطلح المحاكم الرقمية، ويذهب اتجاه إلى أنها المحاكم التي يمارس فيها القضاة أعمالهم من خلال الوسائل الرقمية المتطورة، إلا أننا ندعم الاتجاه القائل بأن هذه الرؤية تعني الخلط بين مفهوم المحكمة الإلكترونية والمحكمة الرقمية، إذ تختص المحاكم الرقمية نوعيًّا بالقضايا ذات الطابع الرقمي والجرائم الإلكترونية والتعاملات الإلكترونية بين الأفراد وفق إطار تشريعي محدد، فهي أحد أنواع المحاكم المتخصصة على غرار محكمة الأسرة والمحكمة الاقتصادية والمحاكم الجنائية المختصة بقضايا الإرهاب، تعمل وفق قواعد إجرائيَّة خاصة تتناسب مع طبيعتها المتخصصة، ويتولاها قضاة متخصصون بنظر هذا النوع من الدعاوى (الحسيني، 2023، ص.241) و(مصري، 2012، ص.88).

وتنظر المحاكم الرقمية الدعاوى المتعلقة بالجرائم المعلوماتية جنائية كانت أو مدنية، كما نرى اختصاصها بهذا النوع من الجرائم وفقًا لمبدأ العينية والعالمية دون التقيد بقواعد الاختصاص الإقليمي؛ نظرًا للطبيعة الاستثنائية لهذا النوع من الجرائم العابر للوطنية، فهي جرائم قد يخطط لها في دولة ويتم تنفيذها في دولة أخرى، ويقع الضرر على المجني عليه في دولة ثالثة، وتكون جنسية مرتكب الجريمة لدولة رابعة.

وهو النهج الذي تبناه المشرع المصري في المادة (3) من القانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات؛ إذ أقرَّ اختصاص القضاء المصري بالجرائم المعلوماتية التي ارتكبت أو تم الإعداد أو التخطيط أو الإشراف عليها، أو تمويلها خارج القطر المصري ولو كان مرتكبها غير مصري، ما دامت قد وقعت إضرارًا بالدولة

المصريَّة وأمنها القومي أو مصالحها أو سلامة أي من مواطنيها أو المقيمين فيها في الداخل والخارج.

وهو نفس الاتجاه الذي أخذت به الاتفاقية العربية لمكافحة جرائم تقنية المعلومات الموقعة في القاهرة 21 ديسمبر 2010 في المادة (3) منها، التي وافقت مصر على الانضمام إليها بموجب القانون رقم 276 لسنة 2014، بالإضافة للمادة (26) من القانون العربي النموذجي لمكافحة جرائم تقنية المعلومات الذي اعتمده مجلس وزراء الداخلية العرب في دورته الحادية والعشرين سنة 2004.

المحاكم الافتراضية

دفع التحول الرقمي في منظومة القضاء بعض الدول نحو الاتجاه إلى استحداث مفهوم المحكمة الافتراضية، وهي محكمة يقصد بها منظومة رقمية تعمل بشكل آلي دون تدخل من البشر عن طريق مجموعة من تطبيقات الذكاء الاصطناعي.

وكانت المملكة العربية السعودية هي أولى الدول العربية التي استحدثت هذا النوع من التقاضي، فاستحدثت «المحكمة الافتراضية للتنفيذ» سعيًا وراء تحقيق العدالة الناجزة وسرعة رد الحقوق، ويتم العمل خلالها آليًّا تحت إشراف قضائي مباشر للتأكد من جودة العملية القضائية، واختصرت المحكمة إجراءات التنفيذ من 12 خطوة إلى خطوتين فقط.

وتتميز المحكمة الافتراضية للتنفيذ وفقًا للنظام السعودي، بسرعة التنفيذ وقبول وتدقيق الطلبات بشكلٍ آلي، ومن ثم إحالة الطلب بعد تدقيقه آليًّا إلى دائرة التنفيذ بالمحكمة، وصولًا إلى إصدار الإجراءات التنفيذية؛ لإكمال عملية التنفيذ.

وتُعدُّ المحكمة الافتراضية تطبيقًا جديدًا للمحاكم الإلكترونية في مجال التقاضي، تتم فيها إجراءات التقاضي آليًا بشكل كامل، وصولًا لصدور الحكم النهائي في الدعوى، إلا أنه لا يمكن أن يتصور أن تعمل هذه المحاكم بعيدًا عن الإشراف البشري وبإدارة كاملة من تطبيقات الذكاء الاصطناعي، فيجب أن يسير العمل بها وفق كافة الضمانات المتعلقة بسير الدعوى وضمانات المتهم في مرحلة المحاكمة، فإن كانت إجراءات الدعوى بالكامل تتم آليًّا فإن قرارها النهائي يجب أن يصدر بعد مراجعة من القضاة الطبيعيين.

2. 3. المطلب الثالث: مفهوم الأمن السيبراني

لا شك أن الأمن السيبراني والهجمات السيبرانيَّة قد أصبحت مصطلحات متداولة ومعروفة لدى مستخدمي الفضاء السيبراني، فأصبح الأمن السيبراني هدفًا أساسيًّا في عالم متطور بشكل سريع غير مسبوق؛ ما دفع جميع الدول نحو اتباع إستراتيجيات وتدابير احترازية تمكنها من مواجهة أخطار الهجوم السيبراني، بما يكفل قدرًا كبيرًا من أمن البيانات والمعلومات.

تعريف الأمن السيبراني

عرف الأمن السيبراني بأنه إجراءات تشمل تخصيص الموارد البشرية والتقنية لحماية النطاق الإلكتروني وأنظمة المعلومات التي تتيح التفاعل داخل هذا النطاق؛ وذلك من أجل منع انتهاكات الخصوصية أو البيانات أو المعلومات الحساسة.

يُطلق على الأمن السيبراني أيضًا مصطلحات مثل: «أمن تكنولوجيا المعلومات» أو «أمان الحاسوب» وهو يشير إلى الإجراءات والعمليات المتَّبعة لحفظ البيانات، والمعلومات والأنظمة الحاسوبية وموارد الحوسبة، بالإضافة إلى أجهزة الاتصال والمعلومات المستخدمة في التخزين، من التعرض للاستخدام غير المرخص أو التغيير أو الإتلاف أو كشف سريتها (مقال منشور الهيئة العامة المصريَّة للاستعلامات، 2023).

مفهوم الهجمات السيبرانيَّة

تعد الهجمات السيبرانيَّة هي محاولات غير قانونية وغير مشروعة للدخول أو التسلل إلى الأنظمة الرقمية أو أجهزة الكمبيوتر أو البنية التحتية للشركات أو الدول أو بيانات الأفراد، بغرض تغيير أو تعديل أو محو أو تدمير المعلومات المخزنة بها أو تعطيل العمل بهذه الأنظمة أو حجب الوصول إليها، على نحو قد يؤدي إلى تسريب معلومات سرية قد تهدد الأمن القومي والاقتصادي والاجتماعي، وتنتج عنه خسائر فادحة، ويشن تلك الهجمات الأفراد وفقًا للمفهوم التقليدي إلا أنه مؤخرًا أصبح الهجوم السيبراني هو أحد أخطر الأسلحة التي تستخدمها الدول فيما يعرف بـ «الحروب السيبرانيَّة».

كما يصنف مكتب التحقيقات الفيدرالي الحادث السيبراني كأي عملية اختراق أو سلسلة من التدخلات الفعلية أو المحتملة، أو تهديدات قادمة، قد تعكر صفو الخصوصية أو تعتدي على سلامة أو توافر البيانات الإلكترونية، إضافة إلى الأنظمة والخدمات والشبكات المتعلقة بها (McLaughlin, 2018, p18,19).

ويشير مفهوم الحرب السيبرانيَّة إلى النزاعات التي تتم من خلال استخدام الكمبيوترات وشبكة الإنترنت، والتي تقوم بها الدول ضد أعدائها، وتُشن هذه الحروب عادةً ضد الشبكات الحكومية والعسكرية للتدخل في عملها، أو إحداث الدمار بها، ويجب عدم الخلط بين الحرب السيبرانيَّة مع الإرهاب السيبراني، أو الجرائم الإلكترونية؛ فعلى الرغم من وجود تقاطع في التقنيات المستخدمة في

كل منها، هناك فروق جوهرية، فوجود حادثة تجسس سيبراني أو هجوم إرهابي سيبراني لا يعني بالضرورة أن دولة ما في حالة حرب سيبرانية، وردًا على القانون الدولي الإنساني تمثل الحرب السيبرانيَّة تطورًا للحروب التقليدية؛ حيث يتم استخدام الأفراد، سواء المدنيون أو العسكريون لمهاجمة شبكات المعلومات فيما يتعلق بنزاع مسلح بين طرفين أو أكثر (عبد الحميد، 2023) و(جيلالي، مراد، 2023، ص.175).

3. المبحث الثاني: جهود الدولة المصريَّة في مجال قوانين الأمن السيبراني

سعت الدولة المصريَّة إلى مواكبة التطور التكنولوجي في جميع المجالات عامة، وفي المنظومة القضائية خاصة، وخلال هذا التوجه لم يغفل المشرع المصري عن وضع الأطر التنظيمية لاستخدام التكنولوجيا ووضع الضوابط المنظمة لها وفق قواعد إجرائية وموضوعية توضح أركان الجرائم السيبرانيَّة، وتتبع وضبط مرتبكي هذا النوع من الجرائم، وتوضيح ما يعرف بالدليل الرقمي وبيان ماهيته، حتى لا نجد أنفسنا أمام سلوك إجرامي رقمي يقع خارج نطاق التجريم، بما يتيح اتخاذ تدابير أمنية قوية وفعَّالة وتوفير حماية أفضل للأنظمة الرقمية والمعلومات الحساسة.

ولكن مع ذلك ما زال استخدام تطبيقات الذكاء الاصطناعي وما يواجهه من تحديات وما يحتمل أن ينتج عنه من جرائم ذات طبيعة استثنائية، بعيدًا عن نطاق التجريم في التشريع المصري حتى الآن - كما في حالة الجرائم المرتكبة في الميتافيرس- وتُعدُّ الجهود التنفيذية والمؤسسية للدولة المصريَّة في مواجهة استخدام التكنولوجية أكثر تطورًا، وتسبق إلى حد كبير الأطر التشريعية، وسنتناول في هذا المبحث الإطار الدستوري والقانوني لاستخدام التكنولوجيا، كما نتناول الجهود التنفيذية والمؤسسية للحد من خطورة هذا التطور وتحقيق الاستفادة المرجوة منه على النحو التالي:

1.3. المطلب الأول: الإطار التشريعي لاستخدام التكنولوجيا الحديثة

اتخذ المشرع المصري العديد من الخطوات الدستورية والقانونية التي تُعدُّ الأساس القانوني لمواجهة الجرائم السيبرانيَّة، والمشكلات المحتملة من التطور التكنولوجي في شتى المجالات سنتناولها على النحو الآتي:

الإطار الدستوري

فرض الدستور المصري لسنة 2014 لأول مرة على الدولة حماية الفضاء السيبراني فقضت المادة (31) منه، بأن أمن المعلومات جزء رئيس في الأمن القومي والاقتصاد، ويجب على الدولة اتخاذ جميع الإجراءات التي تكفل الحفاظ عليه وفقًا للإطار القانوني المحدد لذلك.

كما اعتبرت المادة (68) من الدستور أن الحصول على المعلومات هو حق يكفله الدستور لكل مواطن، ويجب على الدولة توفيرها وإتاحتها، كما تلتزم الدولة بحماية المعلومات والبيانات وضمان سريتها وحفظها وفق الضوابط التي يحددها القانون.

كما تلتزم الدولة وفقًا لنص المادة (69) من الدستور بحماية حقوق الملكية الفكرية بشتى أنواعها، وفي كافة المجالات، خاصة مع اتساع الفضاء السيبراني، وتعدد أدوات ووسائل النشر خاصةً النشر الرقمي.

الإطار القانوني

استجابة للالتزامات الدستورية اتجه المشرع المصري إلى إصدار حزمة من القوانين المتعلقة بالأمن السيبراني والجريمة الإلكترونية نتناولها كما يأتي:

- قانون مكافحة الإرهاب رقم 94 لسنة 2015: ويُعدُّ هذا القانون هو خطوة مهمة استثنائية في سياسة المشرع المصري في مواجهة الجرائم الإرهابية وفق قواعد إجرائية وموضوعية تتناسب مع الطبيعة الخاصة لهذا النوع من الجرائم، فنصت المادة (15) على تجريم استخدام التنظيمات الإرهابيَّة لوسائل الاتصال السلكية أو اللاسلكية أو الإلكترونية، كما عاقبت المادة (20) على جريمة إخفاء أو إتلاف دليل رقمي من شأنه كشف أدلة ارتكاب الجريمة وضبط فاعليها، وقضت المادة (29) من ذات القانون بعقاب كل من أنشأ أو استخدم شبكات الاتصالات أو الإنترنت للترويج للمعتقدات، أو الأفكار الإرهابية أو التأثير على سير العدالة، كما جرَّم ذات النص الدخول غير المشروع للمواقع الإلكترونية الحكومية بغرض الحصول على البيانات، أو المعلومات الموجودة عليها أو تزييفها أو كشف سريتها أو تعديلها بغرض ارتكاب جريمة إرهابية.
- قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018: وتناول هذا القانون تعريف البيانات والمعلومات الإلكترونيَّة، وبيان الالتزامات الواقعة على مقدمي الخدمة، والخروج على مبدأ الإقليميَّة في النصوص الجنائيَّة، والتعاون الدولي في مكافحة الجريمة المعلوماتيَّة، وقواعد وإجراءات حجب المواقع والتظلم من القرارات الصادرة في هذا الشأن، والمعدات والوسائط والدعائم الإلكترونيَّة للنظام المعلوماتي، وطبيعة

الدليل الرقمي ودوره في الإثبات، وتضمن الباب الثالث من هذا القانون أركان الجرائم المعلوماتية والعقوبات المقررة لها، والأساليب المتبعة في ارتكاب هذا النوع من الجرائم وصولًا لضبط مرتكبيها.

ويضع هذا القانون الأساس التشريعي للسيطرة على الكيانات الإرهابيَّة والإرهابيين وجرائمهم الإلكترونية وإنزال العقوبات على مرتكبي تلك الجرائم، مع تحقيق التوازن بين مكافحة الإرهاب، وحفظ الأمن العام، دون الافتئات على الحقوق والحريات التي كفلها له الدستور (العقبي، 2023، ص. 493).

- القانون رقم 146 لسنة 2019 بتعديل بعض أحكام قانون إنشاء المحكمة الاقتصادية رقم 120 لسنة 2008: أطلق هذا التعديل المرحلة الأولى من رقمنة المحكمة الاقتصادية؛ إذ تضمن إجراءات التقاضي الرقمي، وحق المتقاضين في رفع الدعوى إلكترونيًّا وتنظيم إقامة وسير الدعوى وإخطار الخصوم بالحضور إلكترونيًّا.
- قانون حماية البيانات الشخصية رقم 151 لسنة 2020: ووفقًا لنص المادة الثانية تسري أحكام هذا القانون على كل من ارتكب أيًّا من الجرائم المنصوص عليها فيه، سواء أكان مصريًّا أم غير مصري، وسواء أكان مقيدًا في الداخل أو الخارج، وتمتد الحماية المقررة قانونًا إلى الجرائم التي تقع على البيانات الشخصية خارج البلاد، متى كان معاقبًا عليها وفقًا لقانون الدولة التي وقعت فيها، ووفقًا لنص المادة الخامسة من ذات القانون تختص المحاكم الاقتصادية بنظر الجرائم المنصوص عليها في هذا القانون.

وأوضح القانون مفهوم البيانات الشخصية والبيانات الحساسة، وأمن البيانات وبيان ماهية خرق وانتهاك البيانات، كما بين الضوابط التي يلتزم بها المتحكم في البيانات والمعالج لها، وبين الفصل الرابع التزامات المسؤول عن حماية البيانات الشخصية، كما بين القانون مفهوم البيانات الشخصية العابرة للحدود، وأوضحت المواد من (35) إلى (48) أركان الجرائم التي تقع على البيانات الشخصية والعقوبات المقررة لها.

ونضيف إلى القوانين ذات الصلة بالأمن السيبراني في مصر، قانون حماية الملكية الفكرية رقم 82 لسنة 2002 وتعديلاته وقانون تنظيم الاتصالات رقم 10 لسنة 2003، بالإضافة للقانون رقم 71 لسنة 2021 الذي أضاف المادة (168 مكررًا) إلى قانون العقوبات المصري التي تجرم تصوير أو إذاعة جلسات المحاكمات الجنائية عبر الوسائل الإلكترونية، فضلًا عن القانون رقم 141 لسنة 2021 والقانون رقم 185 لسنة 2023 باستبدال نص المادتين (306 مكررًا أ) و(306 مكررًا ب) من قانون العقوبات، إذ أقر المشرع بموجب هذا التعديل عقوبة التحرش الجنسي عبر الوسائل الإلكترونية أو أي وسيلة أخرى.

3. 2. المطلب الثاني: جهود الدولة في مواكبة التطور التكنولوجي

وضعت الدولة المصريَّة خلال سعيها في مواكبة التطور التكنولوجي في كافة القطاعات ودخول عصر التحول الرقمي، سلسلة من السياسات التي تكفل الحماية الكاملة للبيانات المهمة والحساسة، ونتناول في هذا المطلب بعض هذه الجهود على النحو التالي:

- **مدينة العدالة في العاصمة الإدارية:** تأتي ضمن سياسة الدولة المصريَّة بالإسراع في جهود تنفيذ مبادرة (مصر الرقمية)، في إطار السعي إلى مضاعفة قدرات البنية المعلوماتية والرقمية والسعي للاستفادة من تطبيقات الذكاء الاصطناعي في القطاعات كافة. وتشمل مجمعًا مركزيًّا للمحاكم ومركزًا للدراسات، وغيرها من المنشآت الخدمية المختلفة، سيتم تخصيص منطقة ومبنى خاص لكل جهة وهيئة؛ مما يسهم في تسهيل إجراءات التقاضي للمواطن، وتطور من فلسفة العمل بالمنظومة القضائية من خلال عناصر الرقمنة، وتحديث الأدوات التقنية.
- **المجمع المتكامل لإصدار الوثائق المؤمنة والذكية:** يمثل معلمًا تكنولوجيًّا هائلًا مزودًا بأحدث التقنيات لإصدار الوثائق المؤمنة، وهو الأبرز والأكثر تطورًا في هذا القطاع في منطقة الشرق الأوسط وإفريقيا، كما يُعدُّ إضافة كبيرة لتعزيز إستراتيجية الدولة نحو التحول الرقمي والأتمتة، خصوصًا فيما يتعلق بالوثائق والبيانات، والمستندات الخاصة بكافة الهيئات الحكومية.
- **المركز الوطني «للاستعداد لطوارئ الحاسبات والشبكات»** (CERT-EG): تأسس هذا الكيان في عام 2009 بهدف التصدي لمخاطر الإرهاب الإلكتروني وغيرها من التحديات السيبرانيَّة، ويُعنى بتوفير الدعم الفني والميداني للقطاعات الحكومية والمالية، وذلك بإعداد وتقديم التقارير الفنية للهيئات ذات الصلة من أجل الحفاظ على البنية التحتية الرقمية والمعلوماتية، ويركِّز بشكل خاص على قطاعات تكنولوجيا المعلومات والاتصالات والمجال المالي.
- **المجلس الأعلى للأمن السيبراني:** أنشئ بموجب قرار رئيس الوزراء رقم 2259 لسنة 2014، ويعنى بوضع السياسات اللازمة لمواجهة أخطار الهجوم السيبراني، والإشراف على تنفيذها وتحديثها، ويختص بوضع أطر حماية البنية التحتية الرقمية، وتحديد المعايير الملزمة لكل جهة كحد أدنى لتأمين البنية التحتية

الحرجة للاتصالات، ووضع خطط الطوارئ وآليات الرصد والمتابعة الدورية للهجمات السيبرانيَّة.

- **الإستراتيجية الوطنية للأمن السيبراني (2017-2021)**: أطلقها المجلس الأعلى للأمن السيبراني، وتهدف إلى تأمين البنى التحتية الرقمية بشكل كامل في كافة قطاعات الخدمات الرقمية، في إطار سياسة الدولة نحو التحول الرقمي في كافة المجالات.
- **مؤتمر أمن المعلومات والأمن السيبراني «CAISEC'22»** عقد في مصر في يونيو 2022 تحت عنوان «الأمن السيبراني وقت الأزمات»، وناقش المؤتمر مجموعة من القضايا الأكثر أهمية، ومنها ملف الجيل الخامس من الحروب، كما ناقش الأمن السيبراني والمرونة الإلكترونية وبناء وتأمين أنظمة البنية التحتية الحيوية (الهيئة العامة المصريَّة للاستعلامات، 2023).

4. المبحث الثالث: الفرص والتحديات السيبرانيَّة في منظومة التقاضي

كانت الصين هي الدولة الأولى التي تتجه إلى نظام المحاكم الإلكترونية بهدف توفير حل سريع للنزاع وتقليل التكاليف مع ضمان جودة وكفاءة التقاضي، فقد أنشئت في 2017 أول محكمة في العالم يتم التقاضي أمامها عبر الإنترنت من خلال محكمة الإنترنت في «هانغتشو»، تقوم المحكمة بتلقي شكوى المدعي وتفحص الأدلة، ثم تقيد الدعوى وتعلن الخصوم، ويكون حضور أطراف الدعوي إلكترونيًّا عبر الإنترنت، أو عن طريق محاميهم عبر الموقع الرسمي للمحكمة.

وكانت الغاية من تأسيس محاكم الإنترنت في الصين هي تحقيق أقصى استفادة من التطور التكنولوجي لبناء نظام قضائي يتميز بالاحترافية والفاعلية، بالإضافة إلى تقديم خدمة مريحة وموثوق بها لمعالجة القضايا التي تنشأ في الفضاء الإلكتروني بشكل عادل؛ مما يسهم في تحسين جودة وكفاءة عملية التقاضي (Guo, 2021, p.3).

وعلى الرغم من الفرص والإمكانات العديدة التي توفرها الرقمنة في منظومة العدالة وضبط الجرائم ومرتكبيها، فإن هذه الفرص تقابلها العديد من التحديات التشريعية والتقنية، بالإضافة للتحديات المتعلقة بضمانات تحقيق العدالة والخصوصية والتحيز الخوارزمي، وهو ما سنتناوله في هذا المبحث على النحو الآتي:

4. 1. المطلب الأول: الفرص التي توفرها التكنولوجيا في منظومة التقاضي

مما لا شك فيه أن الثورة التكنولوجية والمعلوماتية فتحت المجال أمام تطبيقات عديدة مستحدثة في مجال التقاضي، ونشير إلى بعض هذه الإمكانات كما يأتي:

- استخدام تطبيقات الذكاء الاصطناعي في كتابة القضايا وترتيب أوراقها وتدوين المرافعات ومحاضر الجلسات وتحديد مواعيد الجلسات وفق أولويات ومدى استعجال كل قضية على حدة. فضلًا عن إمكانية كشف التزوير للمحررات المقدمة للمحكمة وإمكانية التحقق من صحة التسجيلات المرئية والمسموعة واستخدام الذكاء الاصطناعي في الإثبات والنفي (الجلعود، 2023، ص. 232).
- يمكن الاستعانة بالذكاء الاصطناعي خلال جلسات المحاكمات في تحليل سلوكيات وردود أفعال الشهود والمتهمين في كل مرحلة من مراحل التحقيق، ويقارن هذه الردود على نحو مستمر لتقديم تقييمات دقيقة وعادلة عن مدى صدق أقوالهم (مقال مترجم من مجلة Forbes، 2021).

كما يمكن للقضاة الاعتماد على الذكاء الاصطناعي للحصول على المعلومات بسرعة وكفاءة، مما يحسن من جودة منظومة التقاضي.

- المعالجة الآلية للبيانات (ADP) تُعدُّ أحد الاستخدامات المهمة للذكاء الاصطناعي، حيث تُظهر فائدتها بشكل خاص في معالجة كميات كبيرة من الوثائق، ولا سيما في عمليات تصنيفها وتحويلها وأرشفتها بطريقة تسهل البحث فيها، بالإضافة إلى الترجمة الآلية؛ إذ تعد مشكلة اللغة من أكبر العقبات التي تواجه منظومة العدالة، فيمكن استخدام تطبيقات الذكاء الاصطناعي في ترجمة الوثائق والمستندات وترجمة المرافعات خاصة في النزاعات التي ينتمي أطرافها إلى جنسيات مختلفة، ويتحدثون لغات مختلفة، مع إتاحة ترجمة الأحكام القضائية إلى لغات مختلفة وفق لغة قانونية متخصصة صحيحة (Elokaby, 2024). كما تُعدُّ أنظمة التلخيص الآلي للبيانات (NPL) أحد أهم الأدوات التي تستخدم في التعاون القضائي الدولي مع ما قد يتوافر من كم كبير من المعلومات، تؤدي تلك الأنظمة دورًا مهمًّا في تقليل وقت الاطلاع عليها ومعالجتها، خاصة القضايا التي تتطلب فيها المعالجة اليدوية وقتًا كبيرًا (Wiewiórowski, Fila, European Union Agency for Criminal Justice Cooperation website).
- لا يقتصر التطور التكنولوجي على رقمنة البيانات والمعلومات والوثائق في العملية القضائية، إنما يمكن أن تمتد قدرات خوارزميات الذكاء الاصطناعي في التنبؤ بالقرارات القضائية في القضايا المنظورة أمام المحكمة عن طريق منظومة التعلم الآلي، وهو ما أطلق عليه البعض «العدالة التنبئية» (كونتيني، مكتب

الأمم المتحدة المعني بالمخدرات والجريمة UNODC)، وإن كنا نرى عدم دقة هذا المصطلح، فالعدالة لا يتنبأ بها إنما يتم الوصول إليها من خلال فحص أوراق الدعوى بما يشكل قناعة القضاة بالحكم قبل إصداره للعلن.

- تقليل التكلفة وتوفير الوقت للمتقاضين والمحامين على حد سواء، فهم يستطيعون الوصول إلكترونيًا للمحكمة، وتقديم الوثائق والمرافعات وحضور الجلسات، دون الحاجة إلى الانتقال للمحكمة (Che-min, 2009, p.241) (Acemoglu, Robinson, 2013, p.183).

بالإضافة إلى تعزيز الشفافية والعدالة من خلال إمكانية الوصول بسهولة لمعلومات وملفات القضية لجميع أطراف الدعوى؛ بما يعزِّز كفاءة ومرونة العملية القضائية وتقليل الأخطاء البشرية المحتملة، وتقليل الازدحام داخل المحاكم (الشريدة، نقابة المحامين المصريَّة، 2023) و(Li & peng, 2023m p.3).

- إصدار الأحكام إلكترونيًا وإتاحة إمكانية الاطلاع عليها على المنصة الإلكترونية للمحكمة، مع تمكين الخصوم أيضًا من الطعن إلكترونيًا على الحكم وفقًا للقواعد القانونية المنظمة لحالات وإجراءات الطعن، ويوضع التقرير بالطعن لقلم الكتاب على الموقع الإلكتروني للمحكمة المختصة، مع توفير أنظمة الدفع الإلكترونية لكافة الرسوم القضائية دون الحاجة إلى التوجه للمحكمة لاستيفائها (الساعدي، 2019، ص. 388-389).
- التحول من النظام الورقي إلى النظام الرقمي في كافة إجراءات التقاضي بداية من رفع الدعوى وإعلان الخصوم وانعقاد الجلسات، ثم الحكم فيها وصولًا لتنفيذ الأحكام إلكترونيًا، بالإضافة لسرعة تطبيق الإجراءات القضائية، وتحقيق إمكانية وصول القضاة لمستندات الدعوى في أي وقت بما يصل في النهاية إلى تحقيق مبدأ العدالة الناجزة الذي كان هدفًا للمشرع، بالإضافة لزيادة الشفافية ومنع الفساد بتقليل تدخل العنصر البشري بشكل كبير(البغدادي، 2022، ص.153-152) و(Veli-cogna, Yein N, 2006, p 370-389).
- استخدام تقنية الفيديو كونفرانس في التحقيق الابتدائي والمحاكمة، على نحو يمكن القضاة والنيابة والخصوم والشهود والخبراء، سواء أكانوا داخل البلاد أو خارجها من حضور الجلسات رغم عدم حضورهم الفعلي داخل المحكمة، فيما يعرف بـ«الحضور الافتراضي» (سالم، 2013، ص. 183) و(Bossan,2011, 804).
- استخدام تطبيقات الذكاء الاصطناعي في المنظومة الأمنية تسهم في تحقق الضربات الأمنية الاستباقية، والتنبؤ بالجريمة ومنع وقوعها، بل كشف مرتكبيها بسرعة ودقة (العبيدي، مقال منشور بصحيفة الرياض، 2014) و(الملا، 2018، ص. 116). وتتبعهم من خلال تطبيقات التعرف على الوجوه وتطبيقات تتبع البيانات البيومترية، بالإضافة للقراءة الذكية لبيانات اللوحات المعدنية للسيارات، واستخدام الخوذة والنظارات الذكية.

ومن التطبيقات المتقدمة للذكاء الاصطناعي في مجال العمل الأمني، نظام مبتكر يستخدم في نيابة دبي يمكنه إصدار أذون القبض والتفتيش خلال دقائق معدودة معتمدًا على التقنيات الذكية، كما تم تدشين الروبوت الشرطي ضمن قوات شرطة دبي، الذي يعد إضافة فنية لتطوير العمل الشرطي، في السياق ذاته، تم تطوير طائرات بدون طيار مزودة بتكنولوجيا قادرة على إبطال مفعول القنابل، وذلك لحماية الخبراء المتخصصين في مجال المتفجرات (عبد الظاهر، مقال منشور بجريدة الوطن، 2018).

وهذه التقنيات وغيرها تمثل ثورة في تحديث الأساليب الأمنية وحماية الأرواح والممتلكات، كل هذه الآليات من شأنها التأثير غير المباشرة على نجاح منظومة العدالة بشكل عام عن طريق منع الجريمة من الأساس وسرعة ضبط مرتكبيها في حالة وقوعها ومحاكمتهم.

4. 2. المطلب الثاني: التحديات التي تفرضها التكنولوجيا على المنظومة القضائية

مقابل ما يتيحه التحول الرقمي من فرص، فإنه يخلق العديد من التحديات (يحيي، 2014، ص. 9)، فالتحديات القانونية هي أخطر المشكلات التي تواجه التحول الرقمي والذكاء الاصطناعي في المنظومة القضائية (القوصي، 2018، ص.7)، وكذلك التحديات المتعلقة بالخصوصية وسرية البيانات، بالإضافة للتحديات المتعلقة بالعلانية وإمكانية الوصول (Hynes, Gill & Tomlinson, 2020, p.8)، وسوف نتناول تلك التحديات بشكل مفصل على النحو التالي:

التحديات القانونية

- عدم مجاراة التطور التشريعي للتطور التكنولوجي، والرغبة في الاتجاه نحو التحول الرقمي وإدخال تطبيقات الذكاء الاصطناعي في منظومة التقاضي (المرزوقي، 2021، ص.257)، وما تستوجب معه من تدخل المشرع بإحداث تعديلات جذرية خاصة من الناحية الإجرائية، على غرار القانون رقم 146 لسنة 2019 بتعديل بعض أحكام قانون إنشاء المحكمة الاقتصادية.

- تحديات التعارض مع المبادئ القانونية الراسخة كمبدأ علانية الجلسات، بالإضافة للتحديات المتعلقة بالشخصية القانونية للروبوتات، وتحديد المسؤول عن أخطاء تطبيقات الذكاء الاصطناعي، فهل تقع المسئولية على مصمم البرنامج أو الشركة المطورة له؟
- التحديات المتعلقة بالاختصاص القضائي بنظر الجرائم السيبرانيَّة؛ نظرًا للطبيعة العابرة للحدود لهذه الجرائم، إذ يجب تحديد الاختصاص بنظرها وفقًا لمبدأ العالمية؛ ضمانًا لحماية مصالح الدولة ومواطنيها في الداخل والخارج، بالإضافة للأجانب المقيمين على أرضها.

التحديات التقنية والاقتصادية

- من المؤكد أن التطور التكنولوجي في منظومة العدالة يتطلب بنية تحتية رقمية ومعلوماتية متطورة، مع ما يترتب على ذلك من تكلفة اقتصادية مرتفعة تقف عائقًا أمام الخطط الموضوعة لمواكبة الاتجاهات العالمية الحديثة في هذا المجال (wang, 2024, p.2).
- تدريب عناصر المنظومة القضائية من قضاة ومحامين والموظفين المتعاملين مع المنظومة الرقمية، بما يضمن رفع كفاءتهم وقدراتهم في استخدام وسائل التقنية الحديثة.
- المشكلات الفنية والأعطال التقنية التي قد تصيب المنظومة الرقمية، سواء أثناء رفع الدعوى أو أثناء تداول الجلسات، وما قد يتجه بنا إلى مشكلات محتملة تتعلق بفوات مواعيد الاستئناف، أو الطعن على الأحكام؛ نظرًا لتعرض الموقع الإلكتروني للمحكمة لمشكلة تقنية.

تحديات إمكانية الوصول

تعدُّ تحديات تكلفة الوصول للعدالة وصعوبة وكثرة الإجراءات المتبعة هي العائق الرئيس الذي يواجه المتقاضين عند محاولة الوصول للمحاكم (Anderson, 2019, p.132)، فالنظام القضائي يجب أن يكون متاحًا للجميع؛ لأن نظام المحاكم غير المتاح أو الذي يصعب الوصول إليه بسهولة وبوضوح لا قيمة له (Cross, C.Donelson, 2010, p 490-510)، لذا أصبح تحسين إمكانية الوصول إلى القضاء هدفًا رئيسًا للابتكار والإصلاح القضائي (Rhode, 2003, p.369) بالإضافة للتحديات المتعلقة بسؤال الشهود وسماع الخبراء عبر الإنترنت (Ghoshray, 2006, p. 338-340).

الدليل الرقمي والأمن السيبراني

وتشكل الأدلة الرقمية تحديًا كبيرًا أثناء التحقيق في الجرائم السيبرانيَّة، فالمشكلات المتعلقة بالأوامر القضائية المناسبة للاطلاع والوصول إلى تلك الأدلة والبيانات، وتقييد الوصول إلى البيانات المتعلقة بالدعوى محل التحقيق بالقدر الضروري والمصرح به دون أن تمتد إلى أي بيانات أخرى بما يشكل انتهاكًا للخصوصية وحريات الأفراد، وتوفير الضوابط الملزمة لمقدمي خدمات الإنترنت والاتصالات بالاحتفاظ بالبيانات وتقديمها للسلطات المختصة عند طلبها، وفقًا للقواعد القانونية الإجرائية المتبعة للحصول على تلك البيانات.

إلا أن المخاوف المتعلقة بالتلاعب بالأدلة الرقمية أو تعرضها للقرصنة أو التزوير أو تعديل محتواها تتزايد بشكل مستمر، بما يدعو الخصوم في الدعوى إلى الدفع بعدم صلاحية تلك الأدلة في الإثبات لعدم ضمان صحتها بما يعرض سلامة العملية القضائية للخطر، كما تُعدُّ صعوبة التحقيق وإمكانية تقديم الدليل المادي الملموس خاصة في الجرائم المتعلقة بتقنية المعلومات، إحدى العقبات في سبيل الوصول للقضاء الرقمي (Granja, Rafael, 2017, p.1).

وهو ما دفع المحاكم الإلكترونية في الصين على سبيل المثال إلى استخدام تقنيات «البلوك تشين» لحماية وتأمين الأدلة الرقمية وضمان عدم التلاعب بها، وكانت محكمة الإنترنت الصينية في «هانغتشو» أول محكمة تؤكد صلاحية استخدام تقنية «البلوك تشين» في حفظ الأدلة الرقمية والاعتداد بصلاحيتها القانونية في الإثبات (Sung, 2020, p.1).

ومع هذا التقدم التكنولوجي في منظومة التقاضي تبرز أخطار الأمن السيبراني والهجمات الإلكترونية، كأحد أكبر التحديات التي تهدد البيانات الشخصية الحساسة وسرية المعلومات القضائية، وهو ما يستتبع التزام الجهات المعنية ببروتوكولات وتدابير أمان كبيرة في الفضاء السيبراني لضمان مواجهة هذه المخاطر، بالتعاون مع الشركات المعنية في مجال الأمن السيبراني من خلال وزارة الاتصالات.

التحديات الأخلاقية (الشفافية والمساءلة)

فمن المؤكد أن توفير آليات قانونية لفهم وفحص مخرجات الأنظمة الرقمية المستحدثة يعزِّز مبدأ الشفافية، بالإضافة لعدم وجود طريقة واضحة لتحليل أساليب الوصول للقرارات القضائية التي خلصت إليها تطبيقات الذكاء الاصطناعي، فضلًا عن صعوبة تحديد المسئولية القانونية في حالة وقوع جرائم أو أضرار ناتجة عن استخدام تطبيقات الذكاء الاصطناعي في المنظومة القضائية.

تحديات التحيز الخوارزمي

فالتحيز المتوقع حدوثه في تطبيقات الذكاء الاصطناعي يُعدُّ عقبة كبيرة من شأنها التشكيك في مصداقية العملية القضائية، فربما يقع هذا التحيز بشكل عمدي من خلال مصممي ومطوري الأنظمة الرقمية أثناء إعداد البرامج ضد فئة معينة أو طائفة معينة أو عدم المساواة (Sereno, 2020, p.680:683) (Gardes, 2021, p.115)، وقد يكون التحيز بشكل غير مقصود ناتج عن آلية التعلم الذاتي للخوارزميات من خلال السوابق القضائية، وعدم مجاراة تلك الخوارزميات للتطورات التشريعية الجديدة والاتجاهات الفقهية والقضائية الحديثة.

تحديات الخصوصية

نشير مثلًا إلى أن إذن النيابة العامة المتعلق بالأدلة الرقمية متى تم بشكل غير صحيح أو تجاوز حدود الجريمة محل التحقيقات من شأنه أن يعرض خصوصية الأفراد وحقوقهم للخطر؛ ومن ثمَّ يجب أن تشمل المنظومة التشريعية الحديثة الضوابط والإجراءات المنظمة لحدود إذن النيابة العامة بما يضمن ضبط مرتكبي الجريمة دون الافتئات على حقوق الأفراد وحرياتهم.

5. النتائج

تناولنا في هذا البحث مجموعة من المفاهيم الحديثة التي ظهرت في المنظومة القضائية وأشرنا إلى تعريف المحاكم الإلكترونية، والمقصود بالمحاكم الرقمية والافتراضية، بالإضافة لمفهوم الذكاء الاصطناعي والأمن السيبراني وتأثيرهما على منظومة العدالة، ثم تناولنا جهود الدولة المصريَّة التشريعية والمؤسسية لمواكبة هذا التطور، والفرص والتحديات التي يفرضها التحول الرقمي على منظومة التقاضي.

وانتهينا من دراستنا إلى أن:

- التحول الرقمي في المنظومة القضائية والأمنية أصبح يفرض نفسه بشكل لا مفر منه، وأضحى لزامًا على المشرع المصري مواكبة هذا التطور، ولا يمكن الاعتماد على أساليب القضاء التقليدي مواكبة للتطور العالمي في هذا المجال.
- التطور التكنولوجي يوفر العديد من الفرص في المنظومة القضائية بما يتيح سهولة وصول المتقاضين والمحامين والقضاة للعدالة وبتكلفة أقل، إلا أنه على الجانب الآخر تفرض تكنولوجيا الذكاء الاصطناعي العديد من التحديات التشريعية والتقنية والاقتصادية فضلًا عن التحديات الأخلاقية.
- عدم مواكبة المنظومة التشريعية الموضوعية والإجرائية للتطور في المنظومة القضائية، فضلًا عن التعارض مع المبادئ القانونية الراسخة كمبدأ علانية الجلسات.

6. التوصيات

- ضرورة تدخل المشرع بمنظومة تشريعية خاصة من الناحية الإجرائية تمثل تعديلًا جذريًّا للإجراءات المتبعة في التقاضي الإلكتروني على غرار النظام المعمول به في المحاكم الاقتصادية، بالإضافة لتطوير تشريعات الأمن السيبراني والجرائم المعلوماتية.
- ضرورة تدخل المشرع بإصدار قانون خاص بالذكاء الاصطناعي، يتضمن قواعد موضوعية وإجرائية حديثة تتناسب مع الطبيعة الاستثنائية للتحديات المتوقعة من استخدام هذا النوع من التكنولوجيا.
- تعزيز قدرات البنية التحتية في المحاكم والنيابات وأقسام الشرطة بما يسهم بشكل كبير في تحقيق الربط الرقمي بين كافة عناصر المنظومة القضائية والأمنية.
- تدريب القضاة والمحامين والموظفين المتعاملين مع المنظومة القضائية، لتحقيق أكبر قدر من الاستفادة من التطور التكنولوجي ومواجهة التحديات المتوقعة نتيجة لهذا التطور.
- تعزيز التعاون الدولي الأمني والقضائي في مجال الأمن السيبراني؛ نظرًا للطبيعة الاستثنائية لهذا النوع من الجرائم العابرة للحدود.

الإفصاح عن تضارب المصالح

يعلن المؤلف أنه ليس له أي تضارب في المصالح للمقالة المنشورة.

الإفصاح عن تمويل البحث

يعلن المؤلف بأن البحث المنشور لم يتلقَ أي منحة ماليَّة، من أي جهة تمويل في القطاعات الحكوميَّة، أو التجاريَّة، أو المؤسسات غير الربحية.

المراجع

المراجع العربية

إبراهيم، محمد. البغدادي، أحمد. (2022). القضاء الرقمي والمحاكم الافتراضية، مجلة بنها للعلوم الإنسانية، المجلد الأول، العدد الثاني.https://doi.org/10.21608/bjhs.1999.275481

الجلعود، أروي بنت عبد الرحمن. (2023). أحكام تطبيقات الذكاء الاصطناعي في القضاء، الجمعية العلمية القضائية السعودية، مركز قضاء للبحوث والدراسات، الرياض.

الحسيني، حنان. (2023). المحكمة الرقمية والمحكمة الإلكترونية في إطار التقاضي الإلكتروني، مجلة جامعة الملك سعود، كلية الحقوق والعلوم السياسية، المجلد 35، العدد الثاني.

https://doi.org/10.33948/1203-035-002-002

الساعدي، قصي. (2019). التقاضي الإلكتروني، مجلة ميسان للدراسات الأكاديمية، جامعة ميسان، كلية التربية الأساسية، مجلد 18، عدد 35.

https://doi.org/10.54633/2333-018-035-030

العبيدي، صلاح الدين. (2014). مقال «مفهوم الأمن في تقنية المعلومات... النظرة العامة والتقنية»، صحيفة الرياض، الرياض.

العقبي، مصطفى. (2023). جريمة الإرهاب في ضوء قانون الكيانات الإرهابية رقم 8 لسنة 2015، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة.

القوصي، همام. (2018). إشكالية الشخص المسؤول عن تشغيل الروبوت، دراسة تحليلية استشرافية في قواعد القانون المدني الأوروبي الخاص بالروبوتات، مجلة جيل الأبحاث القانونية المعمقة، مركز جيل البحث العلمي، العدد 25. https://doi.org/10.33685/1545-000-025-003

المرزوقي، عبد الله. (2021). التقاضي الإلكتروني (التقاضي الذكي) وإلكترونية التقاضي (القضاء الذكي)، دراسة مقارنة لتشريع دولة الإمارات العربية المتحدة مع بعض الأنظمة العربية والأجنبية، مجلة جامعة الشارقة للعلوم القانونية، مجلد 18، عدد https://doi.org/10.36394/jls.v18.i2.7.2

الملا، إبراهيم. (2018). الذكاء الاصطناعي والجريمة الإلكترونية، مجلة الأمن والقانون، المجلد (26)، العدد الأول، أكاديمية شرطة دبي.

جيلالي، شويرب. مراد، فايزة. (2023). مفهوم الحروب السيبرانيَّة والأمن السيبراني، مجلة الحقوق والحريات، المجلد 11، العدد الأول.https://www.asjp.cerist.dz/en/article/219023

https://doi.org/10.54000/0576-026-001-002

خليفة، محمد. (2018). الذكاء الاصطناعي في مجال التشريع، مجلة دبي القانونية، العدد 28، تصدرها النيابة العامة الإماراتية.

خوالد، أبو بكر. (2019). تطبيقات الذكاء الاصطناعي كتوجه حديث لتعزيز تنافسية منظمات الأعمال، المركز الديمقراطي العربي للدراسات الإستراتيجية والسياسية والاقتصادية، الطبعة الأولى، برلين، المانيا.

سالم، محمد. (2013). مظاهر استخدام التكنولوجيا الحديثة في مجال القانون الجنائي (المراقبة الإلكترونية والتحقيق الجنائي عن بعد)، دار النهضة العربية الطبعة الأولى.

عبد الحميد، أميرة. (2023). الحروب السيبرانيَّة، سلسلة مفاهيم معاصرة، المركز القومي للبحوث الاجتماعية والجنائية، العدد الثاني.

عبد الظاهر، أحمد. (2018). القانون الجنائي في عصر الذكاء الاصطناعي، مقال منشور في جريدة الوطن، على الرابط: https://www.elwatannews.com/news/details/3358273

عبد الكريم، فهيل. (2022). دور التكنولوجيا الرقمية في تحقيق العدالة الجنائية: الفرص والتحديات، مجلة جامعة دهوك، المجلد 25، العدد 2.

https://doi.org/10.26682/hjuod.2022.25.2.47

علاي، عمار. عبد المجيد، محمد. (2023). استخدام تطبيقات الذكاء الاصطناعي في مجال التنبؤ بالجريمة والوقاية منها، مجلة جامعة الشارقة للعلوم القانونية، المجلد 20، العدد 4. https://doi.org/10.36394/jls.v20.i4.12

علي، إبراهيم. الشريدة، مشعل. (2023). تسخير التكنولوجيا لخدمة القانون والقضاء والأفراد (التقاضي الإلكترونيُّ ومنصة ناجز في المملكة العربيَّة السعوديَّة أنموذجًا)، مقالة منشور بالموقع الإلكتروني لنقابة المحامين المصريَّة. https://2u.pw/5JYcqFd

علي، رزق. (2021). انعكاسات التحول الرقمي على السياسة الجنائية المعاصرة، مجلة الدراسات القانونية والاقتصادية، المجلد السابع، العدد الثاني.

https://dx.doi.org/10.21608/jdl.2021.209753

محمود، أشرف. (2020). المحاكم الإلكترونية في ضوء الواقع الإجرائي المعاصر، مجلة البحوث الفقهية والقانونية، جامعة الأزهر، المجلد 32، العدد 35.

https://doi.org/10.21608/jlr.2020.140255

مصري، عبد الصبور. (2012). المحكمة الرقمية والجريمة المعلوماتية: دراسة مقارنة، مكتبة القانون والاقتصاد، الطبعة الأولى، الرياض.

منديل، أسعد. (2014). التقاضي عن بعد: دراسة مقارنة، مجلة الكوفة للعلوم القانونية والسياسية، المجلد 7، العدد https://search.mandumah.com/Record/697307.21

يحيى، عادل. (2014). السياسة الجنائية في مواجهة الجرائم المعلوماتية، دار النهضة العربية، الطبعة الأولى.

المواقع الإلكترونية

الأنشطة المتعلقة بالذكاء الاصطناعي في القضاء، مكتب الأمم المتحدة المعني بالمخدرات والجريمة.

https://cutt.ly/9wN8dexB

الموقع الرسمي للمجلس الأعلى للأمن السيبراني. https://www.escc.gov.eg/index.html

تأثير الذكاء الاصطناعي في المحاماة والقضاء. (2021). مقال مترجم من مجلة Forbes، الأكاديمية الدولية للوساطة والتحكيم. https://2u.pw/oKNqv11

فرانشيسكو كونتيني، الذكاء الاصطناعي: هل هو حصان طروادة جديد للتأثير غير المبرر على الأجهزة القضائية، مكتب الأمم المتحدة المعني بالمخدرات والجريمة UNOCD.

https://2u.pw/23CHiPF

مصر والأمن السيبراني. (2023). الهيئة العامة المصريّة للاستعلامات، المركز الإعلامي، مقالة منشورة . https://2u.pw/RvMGVCj

المراجع الإنجليزية

A. Boden, Margaret. (2018). Artificial Intelligence: A Very Short Introduction, Oxford University Press. https://n9.cl/p0ekt

A. Osoba, Osonde. Welser IV, William. (2017). An Intelligence in Our Image, The Risks of Bias and Errors in Artificial Intelligence, Published by the RAND Corporation, Santa Monica, Calif.

https://www.rand.org/pubs/research_reports/RR1744.html

Acemoglu, Daron. A. Robinson, James. (2013). Economics versus politics: Pitfalls of policy advice. Journal of Economic Perspectives, Volume 27, No 2.

https://doi.org/10.1257/jep.27.2.173

Amankwaa, Aaron. McCartney, Carole.(2018). The UK National DNA Database: Implementation of the Protection of Freedoms Act 2012, National Library of Medicine.

https://doi.org/10.1016/j.forsciint.2017.12.041

Anderson, Dorcas .(2019).The Convergence of ADR and ODR Within the Courts: The Impact on Access to Justice, Civil Justice Quarterly, Volume 38, Issue 1.

https://ink.library.smu.edu.sg/sol_research/2842

B. Cross, Frank. C.Donelson, Dain. (2010). Creating Quality Courts, Journal of Empirical Legal Studies, Volume 7, issue 3.

https://doi.org/10.1111/j.1740-1461.2010.01186.x

Chemin, Matthieu. (2009). Do judiciaries matter for development? Evidence from India. Journal of Comparative Economics, Volume 37, Issue 2. https://doi.org/10.1016/j.jce.2009.02.001

Elokaby, M.A. (2024). Development of cybersecurity laws in Egypt and its impact on the judicial system (Opportunities and challenges). Int. Cybersecur. Law Rev. Vol 5.

https://doi.org/10.1365/s43439-024-00132-2

Gerry, Felicity. Muraszkiewicz, Julia. Iannelli, Olivia. (2018). The drive for virtual (online) courts and the failure to consider obligations to combat human trafficking - A short note of concern on identification, protection and privacy of victims, Computer Law & Security Review, Volume 34, Issue 4.

https://doi.org/10.1016/j.clsr.2018.06.002

Ghoshray, Saby. (2006). Charting the Future of Online Dispute Resolution: An Analysis of the Constitutional and Jurisdictional Quandary, University of Toledo Law Review, Volume 38, Issue1.https://2u.pw/4NzMZyl

Granja, Fernando. Rafael, Glen. (2017). The Preservation of Digital Evidence and its Admissibility in the Court, International Journal of Electronic Security and Digital Forensics, Volume 9, issue 1.

https://doi.org/10.1504/IJESDE2017.081749

Guo, Meirong. (2021). Internet court's challenges and future in China, Computer Law & Security Review, Volume 40, 105522.

https://doi.org/10.1016/j.clsr.2020.105522

Hynes, Jo. Gill, Nick. Tomlinson, Joe. (2020). 'In defense of the hearing? Emerging geographies of publicness, materiality, access and communication in court hearings', Geography Compass, Volume 14, Issue 9, e12499.https://doi.org/10.1111/gec3.12499

J. McLaughlin, Brian. (2018). Adjunct Faculty, Trends in State Courts 2018: Cybersecurity: Protecting Court Data Assets.

Wang, Liyuan. (2024). Application of information technology in judicial field: The development model of online litigation in China, Computer Law & Security Review, Volume 52, 105936.
https://doi.org/10.1016/j.clsr.2024.105936.

Ward, Jenni. (2015). transforming 'Summary Justice' Through Policeled Prosecution and 'Virtual Courts': Is 'Procedural Due Process' Being Undermined? The British Journal of Criminology, Volume 55, Issue 2.https://doi.org/10.1093/bjc/azu077

Wiewiórowski, Wojciech. Fila, Michał. AI and data protection in judicial cooperation in criminal matters, European Union Agency for Criminal Justice Cooperation website.
https://www.eurojust.europa.eu/20-years-of-eurojust/ai-and-data-protection-judicial-cooperation-criminal-matters

المراجع الفرنسية

Bossan, Jérôme. (2011) La visioconférence dans le procès pénal: un outil à maîtriser Dans Revue de science criminelle et de droit pénal comparé, , v4.https://doi.org/10.3917/rsc.1104.0801

Gardes, Delphine. (2021). Le droit à l'emploi face à l'intelligence artificielle, Droit Social. https://shs.hal.science/halshs-03129941

Sereno, Sophie. (2020). Focus sur les discriminations par algorithme. Revue de droit du travail, 11.
https://shs.hal.science/halshs-03015886

https://patimes.org/cybersecurity-protecting-court-data/

L. Rhode, Deborah. (2003). Access to Justice: Connecting Principles to Practice, Journal of Law & Policy, Washington University, Volume 12, Issue 1.
https://openscholarship.wustl.edu/law_journal_law_policy/vol12/iss1/5

Li, Wen. Peng, Qing. (2023). Digital courts and corporate investment in sustainability: Evidence from China، International Review of Financial Analysis، Volume 88, 102682m.

Procopiuck, Mario. (2018). Information technology and time of judgment in specialized courts: What is the impact of changing from physical to electronic processing? Government Information Quarterly, Vol 35, Issue 3.https://doi.org/10.1016/j.giq.2018.03.005
https://doi.org/10.1016/j.irfa.2023.102682

Sung, Huang-Chih. (2020). Can Online Courts Promote Access to Justice? A Case Study of the Internet Courts in China, Computer Law & Security Review Volume 39, 10546.
https://doi.org/10.1016/j.clsr.2020.105461

Taher Abou-eleid, Egyptian Ministry of Justice plan for digital transformation, article, 2020. https://2u.pw/8wv75jT

Velicogna, Marco. Yein N, Gar. (2006). Legitimacy and internet in the judiciary: A lesson from the Italian Courts' websites experience. International Journal of law and information technology, Volume 14, Issue 3. https://doi.org/10.1093/ijlit/eal009