International Journal of Financial, Administrative, and Economic Sciences (IJFAES)

المجلة الدولية للعلوم المالية والإدارية والاقتصادية

IJFAES

Vol. (5), No. (11) November 2026 الإصدار (5)، العدد (11)

المساءلة القانونية عن أضرار الذكاء الاصطناعي والخوارزميات: دراسة مقارنة في المسؤولية الجزائية والمدنية والإدارية بين الاتحاد الأوروبي والإمارات العربية المتحدة

سحر أحمد أبو غنيم

دكتورة في القانون العام، المعهد العالي للدكتوراه في الحقوق والعلوم السياسية والإدارية في الجامعة اللبنانية، لبنان

Sahar.aboughnaim@gmail.com

ملخص

يتناول هذا البحث موضوع "المساءلة القانونية عن أضرار الذكاء الاصطناعي والخوارزميات: دراسة مقارنة في المسؤولية الجزائية والمدنية والإدارية بين الاتحاد الأوروبي والإمارات العربية المتحدة" ويهدف إلى بيان الإطار القانوني المُنظّم لاستخدام البيانات والمعلومات ومُعالجتها، وتحديد الأضرار الَّتي قد تنشأ عن المُخرجات الخوارزمية، ولاسيَّما انتهاك الخصوصيَّة والإضرار بالسُمعة، ونشر المعلومات المُضلِّلة والاحتيال، وانتحال الهويَّة والإفصاح غير المشروع عن البيانات الشخصيَّة.

وقد اعتمدت المنهج الوصفي التحليلي المقارن من خلال وصف وتحليل النصوص التشريعية ذات الصلة، وعن طريق مُقارنة آليات الحماية القانونية والرَّقابة على الجزاءات في النظامين الأوروبي والإماراتي.

كما تناول أحكام المسؤولية المدنيَّة من حيث أركانها، وشروط التَّعويض عن الأضرار الماديَّة والمعنوية، والمسؤولية الإدارية، من حيث الالتزامات التَّنظيمية والرَّقابة والجزاءات، هذا بالإضافة إلى المسؤولية الجنائية من حيث أركان الجريمة، وإسناد الفعل إلى الأشخاص الطبيعيين أو الاعتباريين حسب الفعل.

أمَّا نتائجه فتكون في تعدُّد الأطراف المُشاركة في تطوير أنظمة الذكاء الاصطناعي وتشغيلها واستخدامها، الأمر الذي يجعل المسؤولية أكثر تعقيداً، حيث إنَّ مجرد حُدوث الضَّرر عن مُخرجاتٍ خوارزميَّة لا يكفي وحده لإثبات المسؤولية. إذ يتعيَّن التَّحقُق من الفِعل غير المشروع والضَّرر وعلاقته السببيَّة والقصد الجنائي الذي حدَّده القانون. وأوصى البحث بتطوير التَّشريعات المُنظّمة للمسؤولية عن أضرار الذكاء الاصطناعي، وتعزيز الشفافيَّة والرَّقابة البشريَّة، وتحسين حِفظ الأدلَّة الرَّقمية وإثبات السببيَّة، وتوضيح التزامات المُطورين والمُزودين والمُستخدمين، وتفعيل التعاون بين الجِهات الرَّقابيَّة والقضائية، بما يضمن حماية الحقوق وتحقيق التَّوازن بين الابتكار التكنولوجي والمُساءلة القانونية.

الكلمات المفتاحية: الذكاء الاصطناعي، المُستخدم /المُتصفّح، المسؤولية المدنيَّة، الضَّرر.

International Journal of Financial, Administrative, and Economic Sciences (IJFAES)

المجلة الدولية للعلوم المالية والإدارية والاقتصادية

Vol. (5), No. (11) November 2026 الإصدار (5)، العدد (11)

Legal Liability for Harm Caused by Artificial Intelligence and Algorithms: A Comparative Study of Criminal, Civil, and Administrative Liability in the European Union and the United Arab Emirates

Sahar Ahmad Abu Ghneim
PhD in Public Law, Higher Institute for Doctoral Studies in Law, Political and Administrative Sciences, Lebanese University, Lebanon
Sahar.aboughnaim@gmail.com

Abstract

This research examines the topic of "Legal Liability for Harm Caused by Artificial Intelligence and Algorithms: A Comparative Study of Criminal, Civil, and Administrative Liability in the European Union and the United Arab Emirates." It aims to explain the legal framework governing the use and processing of data and information, and to identify the harm that may result from algorithmic outputs, particularly violations of privacy, damage to reputation, the spread of misleading information, fraud, identity theft, and the unlawful disclosure of personal data.

The research uses a descriptive, analytical, and comparative approach. It describes and analyses relevant legal provisions and compares the legal protection measures, oversight mechanisms, and penalties in the European Union and the United Arab Emirates.

The study also examines civil liability, including its main elements and the conditions for compensation for material and non-material damage. It addresses administrative liability in terms of regulatory obligations, supervision, and penalties. In addition, it examines criminal liability, including the elements of a crime and the attribution of criminal acts to natural or legal persons, depending on the nature of the act.

The findings show that the involvement of multiple parties in developing, operating, and using artificial intelligence systems makes liability more complex. The mere fact that harm results from an algorithmic output is not sufficient to establish liability. It is necessary to determine whether an unlawful act occurred, whether damage was caused, whether there is a causal link between the act and the damage, and whether the legally required criminal intent exists.

The study recommends updating legislation governing liability for harm caused by artificial intelligence, strengthening transparency and human oversight, improving the preservation of digital evidence and the proof of causation, clarifying the obligations of developers, providers, and users, and enhancing cooperation between regulatory and judicial authorities. These measures would help protect rights and achieve a balance between technological innovation and legal accountability.

Keywords: Artificial Intelligence, User /Browser, Civil Liability, Harm.

مقدمة

أدَّت وسائل التواصل الاجتماعي والتكنولوجيا المُتطوّرة إلى الدخول بقوَّة في المُجتمعات، وبات الاعتماد على تقنيات المعلومات والاتصالات بديهي وأساسي، وسبيلاً مثيلاً في الدخول إلى المعلومات، وبديلاً مُميَّزاً عن النُظم الإلكترونية السَّابقة. وبالإشارة إلى وسائل التواصل الاجتماعي، فإنَّها الوسائل الأولى في نقل هذه المعلومات ونشرها للمُتصفّح ليتم بعدها استخدام الذكاء الاصطناعي الذي يُعدّ النظام الحديث القادر على تحليل كمياتٍ ضخمة من البيانات، واستخلاص الإنماء والعلاقات والنتائج والتوصيات؛ سواء أكان الاستخدام أو الوسيلة ذات تأثير مُباشر أو غير مباشر على المراكز الاجتماعية والفرديَّة أو القانونية أو الاقتصادية للأفراد؛ وهذا الأمر على الرُّغم من إيجابياته في تقديم الكم الهائل من المعلومات أو البيانات بصورةٍ حديثةٍ وسريعة، إلَّا إنَّه يطرح إشكاليات قانونية تتعلَّق بالخصوصيَّة أو التَّطرُق للبيانات وانتهاك الحقوق، وأخرى تتعلَّق بالتَّمييز وطرح مسؤولية عن الأضرار النَّاتجة عن المُخرجات الَّتي تُقدّمها هذه الأنظمة الذكيَّة.

تتعدَّد تقنيات الذكاء الاصطناعي ولا تنحصر في برنامجٍ موحَّد، إنما أُطلقت هذه التَّسمية نظراً لتعدُّد التَّقنيات والأساليب الَّتي تنبع من مسألةٍ موحَّدة من ناحية النُظم والمعلومات وأساليب الوصول إليها من خلال الأجهزة الحديثة، وتضع مُحرّك البحث المُرتبط بالإنترنت. وقد عرَّفته "منظمة التعاون الاقتصادي والتنمية" UECD بأنَّه "نظامٌ قائمٌ على الآلة، يستنتج في ضوء أهدافٍ صريحة أو ضمنيَّة، ومن المُدخلات الَّتي يتلقَّاها كيفيَّة توليد مُخرجات تتمثَّل في تنبؤات أو محتوى أو توصيات أو قرارات، يمكن أن تؤثر في البيانات الماديَّة أو الافتراضية، مع اختلاف الأنظمة في درجة استقلاليتها وقُدرتها على التكيُّف بعد نشرها". [1]

أمَّا أهمية هذا التعريف، فتَّتخذ خصوصيتها القانونية من ناحية التَّركيز على العلاقة بين المُدخلات والمُخرجات، ودرجة الاستقلالية لأنَّ كُل ذلك من شأنه تحديد المسؤولية عن الضَّرر. كما أنَّ هذا النظام لا يعملُ إلَّا ضمن سلسلةٍ من العمليات بدءاً من البيانات، وانتهاءً بالمُخرجات الَّتي قد يترتَّب عليها آثار واقعية.

يقوم الفرد (المستخدم) بإدخال البيانات إلى هذا النظام، إما عن طريق الحاسوب، أو الهاتف أو الأجهزة الذكيَّة أو الساعة الذكية، وهذا الإدخال يُشكّل مادةً أوليَّة، ويطلب من النظام طرح المعلومات بشأنها، تخضع هذه المعلومات للمُعالجة والتَّحليل وفق نموذجٍ حسابي مُعيَّن، ثُم يُقدّمها النظام بشكل مُخرجات، قد تكون مُجرَّد معلومة أو توصية، أو اتخاذ قرار أو تنفيذ إجراء، وهذا الأمر يؤثر على مُستقبل شخص أو مؤسَّسة أو شركة ويصل إلى مصلحةٍ مُعيَّنة.

وبحسب المعهد الوطني الأميركي للمعايير والتكنولوجيا (NIST) فإنَّ هذه النُظم يمكنها إنتاج تنبؤات أو توصيات أو قرارات، أو تقديم معلومات تؤثر في البيئات الواقعية أو الافتراضية، كما أنَّ المخاطر المُرتبطة بها قد تمُس بالأفراد أو المُنظَّمات أو المجتمع أو البيئة. [2]

ومن ناحية المسؤولية القانونية، ينبغي الإشارة إلى أنَّ فهم الذكاء الاصطناعي يقتضي عدم الوقوف عند المخرج النهائي للنظام، إنَّما العودة إلى المراحل الَّتي أنتجته من مصادر ومعلومات، وعن كيفية إدخالها ثم مُعالجتها، وصولاً إلى النموذج المُستخدم وبيان تدخُّل الإنسان في تشغيل النَّظام أو مُراجعة نتائجه. أمّا الضَّرر فقد ينشأ عن معلومةٍ غير صحيحة، أدخلها أحد مُدخّلي البيانات أو عن معالجةٍ غير سليمة للبيانات، أو لوجود عيبٍ في تصميم النَّظام، أو بسبب اعتماد المُتصفّح على معلوماتٍ غير دقيقة، وهذا ما يُصعّب مسألة تحديد المسؤول عن ذلك.

أمَّا مفهوم الخوارزمية، فإنَّها ترتبط بالعالم "محمد بن موسى الخوارزمي" الذي ارتبط اسمه بتطوير منهجيَّاتٍ حسابيَّةٍ أساسية، وتُعرَّف الخوارزمية Algorithm بأنها "مجموعة مُحدَّدة من خطواتٍ منطقيَّة وحسابيَّة تُحدّد المنهاج لحل مسألةٍ ما". [3]

---

[1]- Organisation for Economic Co-operation and Development (OECD), Explanatory Memorandum on the Updated OECD Definition of an AI System, OECD Publishing, March 2024, No. 8. Accessed on: 1/9/2026. From the below website: https://www.oecd.org/

[2]- National Institute of Standards and Technology (NIST), AI Risk Management Framework (AI RMF) Resources: Executive Summary, Artificial Intelligence Resource Center (AIRC), 2023. From the website below: https://circ.gov/

[3] مجمع اللغة العربية بالقاهرة، (2012). معجم مصطلحات الحاسبات بالمجمع، القاهرة، ط4، ص 27.

ومن النَّاحية الاصطلاحية، تعتبر الخوارزمية إجراءً مُنظماً ومُحدداً يتكوَّن من سلسلةٍ من التَّعليمات أو الخطوات الَّتي تُنفَّذ لمعالجة مُدخلاتٍ مُعيَّنة، بهدف الوصول إلى مخرجٍ أو حلٍّ مُعيَّن. وتعتبر مجموعة من التَّعليمات الَّتي تسمح بإنجاز مهمَّةٍ مُعيَّنة. وهناك خصائص أساسية لها: تحديد الخطوات، قابليتها للتنفيذ، الانتهاء إلى النَّتيجة. [1]

أمَّا ارتباطها بأجهزة الذكاء الاصطناعي فتتمثَّل بمجموعةٍ من القواعد والتَّعليمات الَّتي تُحدّد كيفية مُعالجة المُدخلات للوصول إلى نتيجةٍ مُعيَّنة. ويعمل الذكاء الاصطناعي نماذج وخوارزميات تقوم بتنظيم المعلومات ومُعالجتها واستخلاص النَّتائج منها. وأنَّ دراسة ذلك تُشكّل الأساس الضَّروري لفهم توزيع المسؤوليَّة القانونية عن الضَّرر الخوارزمي، حيث إنَّ تحديد المسؤول يتطلَّب معرفة مصدر الخلل، ومن ثم يتم الانتقال من الجانب التَّقني لتحديد الفرد الذي يترتَّب عليه المُساءلة الإدارية والمدنيَّة والجزائيَّة عن الأضرار. [2]

يرتبط نشاط وعمل الذكاء الاصطناعي والأنشطة الخوارزمية بوصفها تقنيَّة، وتُشكّل مصدراً مُحتملاً للضَّرر ومَحلاً للمُساءلة. والمسؤولية لغةً تعني تحمُّل تبِعَة الفِعل والالتزام بالجواب عنه. أمَّا تعريفها اصطلاحاً فتعني العلاقة القانونية الَّتي تنشأ بين مُرتكب الفِعل غير المشروع، والجزاء أو وسيلة الانتصاف المُقرَّرة قانوناً، وتُعدُّ الرابطة القانونية الَّتي تصِل بين الخطأ ووسيلة جبره أو الجزاء المُترتّب عليه، حيث إنَّ من يرتكب فِعل الخطأ يكون مسؤولاً عنه، وتُمثّل المسؤولية رابطةً قانونية ضرورية بين مُرتكب الخطأ ووسيلة الانتصاف منه. [3]

من النَّاحية القانونية، تتداخل المسؤولية من حيث طبيعتها ما بين إداريةٍ ومدنيةٍ وجنائيةٍ، وتقع على الفرد متى ما توافرت شُروطها وخصائصها، لكنَّ الإشكالية تكون على من تقع المسؤوليَّة إذا لم يكن الضَّرر سببه فعلٌ بشري، لأنَّ الذكاء الاصطناعي يختلف عن النَّشاط التقليدي في أنَّ الضَّرر قد لا يكون نتيجة فعلٍ بشري مُباشر يمكن تحديده بسهولة، إنَّما يكون نتيجة سلسلةٍ تقنيةٍ مُتتابعة، تبدأ بطلب معلومة وتنتهي بمُخرجاتٍ يُقدّمها النَّظام.

مشكلة البحث

تكمُن إشكالية البحث في طرح موضوع المُساءلة القانونية عن أضرار الذكاء الاصطناعي والخوارزميات، حيث إنَّ الإشكالية تكمن عندما يكون مُقدّم الخدمة هو نفسه فرد، فلا يكون مُقدَّم النظام هو من اتخذ القرار النهائي بالاستناد إلى المُخرجات الَّتي حصل عليها من الذكاء الاصطناعي، فالتساؤل يكون حول الشخص الذي تقع عليه المسؤولية القانونية، ومعرفة من هو من بين هؤلاء الأفراد: مُرسل المعلومات، مُطوّر النَّظام، مُقدّم الخدمة، مُشغّل النظام، المُستخدم النهائي. وإذا كانت المسؤولية قابلة لأن تكون مساوية بينهم كلهم، أو على حسب نوع الخدمة الَّتي ساهمت في إحداث الضَّرر. وبحسب قواعد القانون المدني فإنَّ المسؤولية تقوم على إثبات الخطأ والضَّرر ووجود علاقة سببيَّة. وبالنسبة لهذا النوع من الضَّرر فيصعب تحديد الفرد الذي تسبَّب مُباشرةً بهذا الضَّرر.

وتكمن الإشكالية في بيان مدى كفاية القواعد القانونية المُنظّمة للمسؤولية عن الأضرار، والَّتي تظهر في نشاط الذكاء الاصطناعي والخوارزميات، تلك التي تلحق بالأفراد من مرحلة إدخال البيانات حتى إظهار المُخرجات، وبيان التَّشريعات النَّاظمة لهذا الأمر في كُلٍ من الاتحاد الأوروبي والإمارات العربية المتحدة، وتحديداً في مسألة تحديد المسؤول القانوني عن الضَّرر وتلك المسؤوليات المدنية والإدارية والجنائية؟

ويتفرَّع عن الإشكالية عدَّة أسئلة منها:

- ما طبيعة المعلومات والضَّرر الناشئ عنها؟
- تحديد الأضرار النَّاشئة عن المُخرجات الخوارزمية؟

[1]- Stanford Encyclopedia of Philosophy, "The Philosophy of Computer Science," 2013. Accessed on: 1/9/2026. From the website below: https://www.plato.stanford.edu/

[2]- Elham Tabassi, Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1, National Institute of Standards and Technology, Gaithersburg, Maryland, 2023.

[3]- Salmond, John W., Jurisprudence, 4th ed., Stevens and Haynes, London, 1913, available on Scribd. Accessed on: 1/9/2026. From the website below: https://www.scribed.com/

- ما مسؤولية الشخص الذي يُرسِل معلومات ويُدّخِل بيانات غير صحيحة إلى النَّظام، والأضرار النَّاشئة عنها؟
- كيفية مُعالجة قواعد المسؤولية المدنيَّة والإدارية والجنائية في إثبات الأضرار الخوارزمية؟
- ما مدى كفالة حماية قواعد البيانات الشخصية للمُتضرّر عندما يكون الضرر ناتجاً عن مُعالجة بياناته بواسطة الذكاء الاصطناعي؟
- ما خصوصية الأضرار الخوارزمية في تطوير قواعد المُساءلة وإذا كانت ضمن قواعد المسؤولية تتنوَّع ما بين المدنية والإدارية والجنائية؟

أهداف البحث

- بيان ماهية ومفهوم ومواضع المُساءلة عن أضرار الذكاء الاصطناعي والخوارزميات من خلال تحديد طبيعة الضَّرر من مرحلة طلب المعلومات وصولاً إلى المُخرجات.
- توضيح نطاق المسؤولية القانونية للأطراف المُتداخلة في دورة إدخال المعلومات واستخدامها في الذكاء الاصطناعي.
- إظهار أساس المسؤولية المدنية والإدارية والجنائية ومُشكلة تحديد عدم اكتمال قواعد المسؤولية.
- تحديد ومقارنة الأُطر القانونية النَّاظمة للمُساءلة في هذا المجال في كُلٍ من الاتحاد الأوروبي والإمارات العربية المتحدة.
- تقدير القواعد القانونية القائمة في حماية المُتضرّرين من أضرار الذكاء الاصطناعي.

أهمية الدراسة

تكمن أهمية هذا الموضوع بالنَّظر إلى حداثتِهِ والاعتماد شبه الكُلّي على الذكاء الاصطناعي في مُختلف جوانب الحياة، والأعمال الأساسية الَّتي تتطلَّب اطلاع ومعرفة مُوسَّعة، وتسييراً لأمور العمل؛ ونظراً لِمَا يتم تداوله وسُرعة انتشاره، وتناقُله بين الأفراد على اختلاف أعمارهم، وبسبب عدم مُراعاة مستوى مُعيَّن من المُخرجات المُقدَّمة للأفراد؛ الأمر الذي أدَّى لِحُدوث تمييز وتشهير للبعض منهم وتناقُل المعلومات بشكلٍ يُضر بالمُستخدمين في بعض الأحيان، ممَّا استدعى تسليط الضَّوء على موضوع المسؤولية عن الأضرار النَّاتجة عن الذكاء الاصطناعي والانخراط بالخوارزميات المُرتبطة بالتحوّل الرَّقمي المُعاصر.

وعليه نُشير إلى مجموعةٍ من النقاط المُهمَّة المُتعلِّقة بالدراسة، وهي:

- بيان الآثار القانونية المُترتّبة على الانتشار المُتسارع للذكاء الاصطناعي في مراحل ومجالاتٍ مُتعدِّدة تمُس حياة الأفراد وحقوقهم ومصالحهم.
- مُعالجة إشكالية قانونية جديَّة تمَّ التطرُّق لها وتنظيم المسؤولية بشأنها بشكلٍ واضح في تشريع الاتحاد الأوروبي، وبعض الدُّول الَّتي أخذت بأهميته بما فيها الإمارات العربية المتحدة.
- التَّركيز على دورة البيانات والمعلومات وصولاً إلى المُخرجات، مع صعوبة تحديد المسؤولية القانونية لِكُل طرف في هذه المرحلة عند حُدوث الضَّرر.
- استشراف هذه الدراسة للمُستقبل، حيث إنَّ حداثة الأنظمة التِّكنولوجية تستدعي الإضاءة على المُشكلات التي تطالُها، وتحديد الطَّرف الذي يتحمَّل المسؤولية عن الضَّرر عند حُدوثه.

محتويات الدراسة

ملخص.

مقدمة.

الفصل الأول: الإطار القانوني للمسؤولية عن البيانات والمعلومات في أنظمة الذكاء الاصطناعي:

- المبحث الأول: مفهوم طبيعة المعلومات والضرر الناشئ عنها.

- المبحث الثاني: الأضرار الناشئة عن المخرجات الخوارزمية.

الفصل الثاني: المسؤولية المدنية والجنائية والإدارية عن أضرار الذكاء الاصطناعي مقارنة بين الاتحاد الأوروبي والإمارات العربية المتحدة:

- المبحث الأول: المسؤولية المدنية والتعويض.
- المبحث الثاني: المسؤولية الإدارية والجزاءات والرقابة.
- المبحث الثالث: المسؤولية الجنائية وإسناد الجريمة.

خاتمة.

حدود الدراسة

تتنوَّع حُدود الدراسة بالنسبة لموضوع البحث المطروح وهي:

1. موضوعية: إذ تتطرَّق لموضوع عالمي يشرح المُشكلة من النَّاحية الأولى، ثُمَّ يتخصَّص من ناحية التَّشريعات، وصولاً إلى تحديد المسؤولية ما بين مدنيَّة وجزائية وإداريَّة.
2. مكانية: بما أنَّ الموضوع عالمي، فالفائدة تكون لِكُل من يتصفَّح ويستخدم أنظمة الذكاء الاصطناعي، أمَّا خصوصيتها فتكون وفقاً لِمَا تطرَّق له التَّشريع الصَّادر عن الاتحاد الأوروبي، والآخر عن الإمارات العربية المتحدة.
3. قانونية: وفق التَّشريع الصَّادر عن كُلٍ من الاتحاد الأوروبي والإمارات العربية المتحدة من ناحية تحديد قواعد المسؤولية عن أضرار الذكاء الاصطناعي، والقانون المرسوم الاتحادي بشأن حماية البيانات والمعلومات.
4. زمنية: مُرتبطة بالعصر الرَّقمي والتَّشريعات الحالية وجداولها، ومدى إمكانية تطوّرها في تطور مفهوم المسؤولية، والقدرة على استيعاب الأضرار الخوارزمية الحديثة.

منهج الدراسة

تعتمد هذه الدراسة على المنهج الوصفي التَّحليلي المُقارن، إذ تمَّ استخدام المنهج الوصفي لبيان المفاهيم الأساسية لهذا الموضوع وتحديد الأضرار والأطراف المُتداخلة فيه.

أمَّا المنهج التحليلي فاعتمد على تحليل النُّصوص التَّشريعية والقواعد القانونيَّة النَّاظمة وتلك المُتعلِّقة بالمسؤولية المدنيَّة والجزائية والإدارية، وكذلك مدى إمكانية تطبيقها عن الأضرار النَّاتجة عن أنظمة الذكاء الاصطناعي والضَّرر الناشئ عنها. أمَّا المنهج المقارن فيعتمد بين الاتحاد الأوروبي وموقف الإمارات العربية المتحدة في تنظيم المسؤولية، ضمن دورة التَّصفُح من إدخال المعلومات وصولاً إلى المُخرجات.

الإطار النظري والدراسات السابقة

الدراسات باللغة العربية:

1. خالد محمد أحمد، (2026). المسؤولية القانونية للذكاء الاصطناعي والقانون الواجب التطبيق عليها، مجلة جامعة الأنبار للعلوم القانونية والسياسية، جامعة الأنبار، السنة 16، العدد 2، ص 572 – 591:

   اعتمدت هذه الدراسة على المنهج الوصفي والتحليلي، وخلصت إلى صعوبة استيعاب التشريعات القائمة للخصائص القانونية والتقنيَّة للذكاء الاصطناعي، والحاجة إلى تنظيم قانوني أكثر مُلاءمة. وأوصت بتطوير القواعد القانونية وتحديد القانون الواجب التَّطبيق على المُنازعات الناشئة عن الذكاء الاصطناعي.

2. سعد عبدالله الهاجري، (2026). المسؤولية المدنية عن أضرار الذكاء الاصطناعي بين التعاقدية والموضوعية: مقارنة بين التشريعات العربية والاتحاد الأوروبي (2021 -2025): دراسة تحليلية نقدية. مجلة العلوم الاقتصادية والإدارية والقانونية، المؤسسة العربية للعلوم ونشر الأبحاث، المجلد 10، العدد 5، ص 78-93:

   اعتمدت هذه الدراسة على المنهج التحليلي النقدي المقارن، وخلصت إلى صعوبة تطبيق القواعد التقليدية بسبب استقلالية

الأنظمة الذكيَّة وصعوبة إثبات الخطأ والسببيَّة. وأوصت بتطوير قواعد المسؤولية المدنيَّة بما يتناسب مع طبيعة أضرار الذكاء الاصطناعي.

3. عبد الباسط جاسم الفهداوي ونوفل حردان، (2024). نحو تأصيل عصري للمسؤولية المدنية الناشئة عن أضرار تطبيقات الذكاء الاصطناعي. مجلة جامعة الأنبار للعلوم القانونية والسياسية، جامعة الأنبار، السنة 14، العدد 2، الجزء 2:

اعتمدت هذه الدراسة المنهج التحليلي وخلصت إلى صُعوبة تحديد المسؤول عن الأضرار النَّاجمة عن بعض تطبيقات الذكاء الاصطناعي، وبالأخص مع تفاوت مستوى الاستقلالية والرَّقابة البشريَّة، وأوصت بإعادة تأهيل قواعد المسؤولية المدنيَّة بما يتلاءم مع الخصائص التقنيَّة للأنظمة الذكيَّة.

الدراسات باللغة الأجنبية:

1. Buiten, Miriam, (2024). Product Liability for Defective AI, European Journal of Law & Economics, Vol. 57, pp: 239 – 273:

اعتمدت هذه الدراسة المنهج التحليلي القانوني، والتحليل الاقتصادي. وخلصت إلى صُعوبة تحديد عيب أنظمة الذكاء الاصطناعي بسبب اختلاف السيطرة والوعي بالمخاطر بين المُنتِج والمُستخدم. وأوصت بربط معيار العيب بدرجة السيطرة على مخاطر النظام وتوزيع المسؤولية وفقاً لذلك؟

2. Guido Noto La Diega & Leonardo C. T. Bezerra, (2024). Can There Be Responsible AI Without AI Liability? Incentivizing Generative AI Safety Through Ex – Post Tort Liability Under the EU AI Liability Directive. International Journal of Law & Information Technology, Vol. 32, Article 021:

اعتمدت هذه الدراسة المنهج التحليلي القانوني ووضع نُظم المسؤولية التقصيريَّة، وخلصت إلى صُعوبة إثبات العلاقة السببيَّة، والحصول على الأدلَّة على أضرار الذكاء الاصطناعي. وأوصت إلى تعزيز آليات الكشف عن الأدلَّة، وقواعد إثبات السببيَّة وربط المسؤولية اللَّاحقة بالتَّنظيم الوقائي للذكاء الاصطناعي.

3. Katri Hava, Ruslan Saleev, Didem Polad, Diana Pfau, Tahoora Heydari & Alma Sofia Makelia, (2024). Regulating Liability for AI – Indeed Harm: Developments in EU Law and Insights from a Research Project. Helsinki Legal Studies Research Paper, No. 87, University of Helsinki, pp: 19:

وقد اعتمدت هذه الدراسة على المنهج التحليلي القانوني، وذلك بالاستناد إلى مشروعٍ بحثي حول قواعد المسؤولية في الاتحاد الأوروبي، وخلصت إلى وجود تحديَّات في تطبيق القواعد الحالية وتوحيدها بين الدُّول الأعضاء مع وجود محدوديَّة في التَّعويض عن الأضرار. كما أوصت بتطوير إطار أوروبي أكثر اتساقاً للمسؤولية، والعمل على تحسين آليات مُعالجة الضَّرر وإثباته.

مصطلحات البحث وتعريفاتها

- **الذكاء الاصطناعي:**

مجموعة من الأنظمة الحاسوبية القائمة على مُعالجة البيانات والمُدخلات باستخدام نماذج وخوارزميات، تُمكنّها بدرجاتٍ مُتفاوتة من الاستقلالية، مع استنتاج أو توليد مُخرجات تتمثَّل في معلومات أو محتوى أو تنبؤات أو توصيات أو قرارات، ويمكن أن يترتَّب على استخدامها أثر قانوني أو ضرر مادي أو معنوي للأشخاص. [1]

[1]- European Parliament and Council of the European Union, Regulation (EU) 2024/1689 of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), Official Journal of the European Union, OJ L, 2024/1689, 12 July 2024, Art. 3(1).

- **المستخدم /المتصفح:**

هو الشخص الذي يتعامل مع الذكاء الاصطناعي أو يقوم باستعماله لغرضٍ مُعيَّن، ويُعد كُل شخص طبيعي أو اعتباري يتعامل مع هذا النظام، بإدخال البيانات أو المعلومات إليه، أو الاستعلام منه، أو تلقّي مُخرجاته، أو استخدامها، أو نشرها، أو الاعتماد عليها، متى كان هذا السلوك له أثر في نشوء الضَّرر محل المُساءلة.[1]

- **المسؤولية المدنية:**

الالتزام القانوني الذي يترتَّب على الشخص الطَّبيعي أو الاعتباري الذي أسهم بفعل، أو امتناع أو إخلال بواجب قانوني أو تعاقدي في إحداث ضررٍ مُرتبط عن أنظمة الذكاء الاصطناعي أو المُخرجات الصَّادرة عنه، متى توافرت شُروط المسؤولية والعلاقة السببيَّة حسب القانون ذات الصلة.

- **الأضرار:**

كُل أثر سلبي أو مادّي أو معنوي أو حقوقي يُصِيب شخصاً نتيجة استخدام ذكاء اصطناعي أو مُعالجة البيانات والمعلومات متى أمكن إثبات الضَّرر، وعلاقته بالفِعل أو الامتناع أو المَخرج النَّاتج من الذكاء الاصطناعي محل المُساءلة وفقاً للقواعد القانونية الواجبة التَّطبيق.[2]

وعليه يتكون هذا البحث من فصلين، وهما: الفصل الأول، ويمثل الإطار القانوني للمسؤولية عن البيانات والمعلومات عن أنظمة الذكاء الاصطناعي. الفصل الثاني، المسؤولية المدنية والجنائية والإدارية عن أضرار الذكاء الاصطناعي مقارنة بين الاتحاد الأوربي والإمارات العربية المتحدة.

الفصل الأول: الإطار القانوني للمسؤولية عن البيانات والمعلومات عن أنظمة الذكاء الاصطناعي

أحدث استخدام الذكاء الاصطناعي تحوّلاً جوهريَّاً في تحديد المسؤولية القانونيَّة، حيث إنَّ الضَّرر من استخدامه ليس بمجرَّد نشرها ممَّا يمُسّ بخصوصيَّة الغير. ويندرج إطار الخصوصيَّة في الذكاء الاصطناعي إذا أدَّى إلى إنتاج النتيجة الضَّارة عملٌ فردي، إنَّما يرتبط بسلسلةٍ من الأفعال بدءاً من جمع المعلومات من مصادر متنوعة وصولاً إلى إدخالها في النّظام، وبعدها طلب مُعالجتها، ومن ثم إنتاج المُخرجات، وهذه الأخيرة تدفع بالمُستخدم إلى القيام أحياناً بإعادة نشرها، ممَّا يمُس بخصوصيَّة الغير. ويندرج إطار الخصوصيَّة في الذكاء الاصطناعي إذا أدَّى إلى إنتاج النتيجة الضَّارة مع عددٍ من الأشخاص أو الجِهات من مصدر البيانات ومُدخلاتها، إلى مُطوّر النِّظام ومُقدّم الخدمة والمُشغِل والمُستخدم النهائي. وهذا ما يجعل تحديد المسؤولية أكثر تعقيداً، لأنَّها بمفهومها التقليدي تقوم على الخطأ والضَّرر. وبحسب "المفوضية الأوروبية" فإنَّ التحديات هي لهذه الناحية وبالأخص في تحديد الشخص الذي يمكن إسناد الضرر إليه وإثبات العلاقة السببيَّة بين السُلوك والنَّتيجة.[3]

لا يوجد نظام موحَّد دولياً للمسؤولية المدنيَّة أو الجنائيَّة عن أضرار الذكاء الاصطناعي، إنَّما أنشأت منظومة مُتعدَّدة المستويات تجمع بين قواعد المسؤوليَّة المدنيَّة التقليديَّة وبين التَّشريعات الَّتي تتعلَّق بحماية البيانات وصون الخصوصيَّة، وأخرى تتعلَّق بحماية المُستهلك وكذلك بالأمن السيبراني. وقد وضعت المنظمات الدوليَّة مبادئ إرشادية ذات طبيعة غير مُلزمة أو شبه تنظيميَّة، حيث وضعت "اليونسكو" توصية بشأن أخلاقيات الذكاء الاصطناعي، وهناك نُظم قانونية نصَّت على الانتقال من المبادئ العامَّة إلى تشريعاتٍ مُلزمة ومُباشرة. وهذا الأمر يُظهر عدم اتّخاذ نموذج موحَّد من حيث وضع الإطار القانوني،

[1]- Redka-Ligarska, Iwona, "Employer as an AI System Operator and Tortious Liability for Damage Caused by AI Systems: European and US Perspectives," The Chinese Journal of Comparative Law, Vol. 12, Oxford University Press, 2024, pp. 1–23, from the website below: https://doi.org/10.1093/cjcl/cxae015

[2]- Ernst Karner, Bernhard A. Koch, and Mark A. Geistfeld, Comparative Law Study on Civil Liability for Artificial Intelligence, European Commission, Directorate-General for Justice and Consumers, 2021.

[3]- Ernst Karner, Bernhard A. Koch, and Mark A. Geistfeld, Comparative Law Study on Civil Liability for Artificial Intelligence, Ibid, p: 9 -17.

فالبعض دمج حماية البيانات والمُنتجات والخدمات الرَّقميَّة، وأخرى وضعت قواعد عامَّة للمسؤولية، ممَّا يعكس عدم استقرار النموذج النهائي القانوني للمُساءلة في هذا المجال. [1]

وضع الاتحاد الأوروبي مُقدمة النُظم القانونية للذكاء الاصطناعي، عبر قواعد مُتفرّقة لإنشاء إطار تشريعي وقائم على تقييم المخاطر، إذ صدرت الوثيقة Regulation EU 1689/2024 الَّتي مثَّلت إطاراً موحداً لتنظيم الذكاء الاصطناعي داخل الاتحاد الأوروبي، وفق مستوياتٍ مُختلفة من المخاطر، ووضعت التزامات متفاوتة على مُقدّمي الأنظمة ومُستخدميها وغيرها. كما أنَّ أثرها لم يقتصر على الاستخدامات الخطرة، إنَّما امتدّ إلى فرض مُتطلباتٍ تتعلَّق بإدارة البيانات والشفافيَّة والتَّوثيق والرَّقابة البشريَّة وإدارة المخاطر، ممَّا يجعل الامتثال التَّنظيمي السَّابق جزءاً من المسؤولية القانونية اللَّاحقة. ولا ينظر في هذه الوثيقة إلى الضَّرر باعتباره نتيجةً نهائيةً مُفصَّلة من عملية إنتاجه، إنما يفرض التزامات على المراحل الَّتي يمكن أن ينشأ فيها الخطر. [2]

أوجب قانون الاتحاد الأوروبي للذكاء الاصطناعي استخدام تقنيَّات التَّدريب للنماذج بالبيانات، أن تستند إلى مجموعات بيانات للتدريب والتَّحقُّق والاختبار ذات معايير الجودة، وأن تخضع لمُمارسات مناسبة لحوكمتها وإدارتها مع النَّظر إلى طريقة جمعها، إعدادها، تنظيمها، تحديثها، تجميعها، وفحصها للكشف عن أوجه التَّحيُز الَّتي قد تؤثر في صحَّة الأشخاص أو سلامتهم أو المسّ بحقوقهم الأساسية؛ وهذا الأمر يظهر صِلةً مُباشرة بين حماية البيانات والمسؤولية عن الضَّرر. وإذا تبيَّن أنَّ الضَّرر بسبب بياناتٍ ناقصة أو غير دقيقة أو مُتحيِّزة، أو تمَّ جمعها بصورةٍ غير مشروعة، فإنَّ المسؤولية تقع في المرحلة الَّتي دخلت فيها البيانات إلى النَّظام.

إلى جانب الوثيقة أعلاه، هناك اللائحة العامَّة لحماية البيانات (GDPR) إذ أرست مبادئ المشروعية والإنصاف والشفافيَّة والدّقة، تقليل البيانات، وتحديد مدَّة الاحتفاظ وغيرها من الأمور، حيث إنَّه إذا تم إدخال معلومات غير صحيحة أو الاستمرار بمُعالجة بياناتٍ غير دقيقة، فإنَّه يمكن أن يكون مصدراً مُستقلاً للضَّرر، وبالأخص إذا تمَّ استخدامه في وضع نموذج أو توصية، أو قرارٍ يتعلَّق بالشَّخص محل البيانات. [3]

يُضاف إلى ذلك التَّدابير التقنيَّة والتَّنظيمية المُناسبة، حيث ترتبط بمرحلة تصميم وسائل المُعالجة ذاتها وفقاً لمبدأ حماية البيانات منذ التَّصميم، ممَّا يجعل المسؤولية عن البيانات مُتداخلة مع مسؤولية تصميم النَّظام التَّقني. وقد تنشأ مسؤولية مستقلة عن مُجرَّد النَّتيجة الَّتي يُحدثها الذكاء الاصطناعي وتكشف عن انتقالٍ مُهم من نموذج قانوني ينتظر تحقُّق الضَّرر، ثم البحث المسؤول، ويفرض على هذا الأخير إدارة المخاطر قبل وقوع الضَّرر.

تمنح اللائحة العامة لحماية البيانات (GDPR) الشخص المعني حقوقاً وضمانات في مواجهة بعض صور اتخاذ القرار الآلي والتَّوصيف الشخصي، بما يحُد من تحوَّل القرار الخوارزمي إلى وسيلة تُنتج أثراً قانونياً أو أثراً مُماثلاً على الشَّخص دون ضماناتٍ مُناسبة، حيث يفترض توزيع المسؤولية عن أضرار الذكاء الاصطناعي من ناحية مصدر القرار، اختيار النموذج، المُسيطِر على عملية المُعالجة، مدى صحَّة البيانات وتناسُبِها مع الغرض، ومعرفة إذا كان هناك رقابة بشريَّة فعليَّة. [4]

تكمن الصُعوبة في إثبات المسؤولية من النَّاحية القانونية، حيث إنَّ التَّعقيد المُبيَّن في النظام الخوارزمي، وعدم الشفافيَّة والاستقلاليَّة يُصعّب معرفة المُتضرّر، أي جزء من هذا النظام أدَّى إلى النَّتيجة الضَّارة. كما أنَّ إعادة النَّظر في عبء الإثبات

[1]- Bertolini, Andrea, Artificial Intelligence and Civil Liability, European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, Brussels, 2020, pp. 7–16, from the website below: DOI: https://doi.org/10.2861/220466

[2]- Holtz, Hajo Michael, and Jonas Ledendal, "AI Data Governance – Overlaps Between the AI Act and the GDPR," Law, Innovation and Technology, Vol. 18, No. 1, 2026, pp. 380–409, from the website below: https://doi.org/10.1080/17579961.2026.2633677

[3]- Holtz, Hajo Michael, and Jonas Ledendal, "AI Data Governance – Overlaps Between the AI Act and the GDPR," Ibid.

[4]- Holtz, Hajo Michael, and Jonas Ledendal, "AI Data Governance – Overlaps Between the AI Act and the GDPR," Ibid.

قد يكون ضرورياً لضمان حُصول المُتضرّر على التَّعويض. [1]

أمَّا في الإمارات العربية المتحدة، فإنَّ التَّنظيم القانوني يختلف عن النموذج الأوروبي في نقطةٍ أساسية، ولا يوجد تشريع شامل موحَّد حتَّى الآن بشأن الذكاء الاصطناعي، يقوم الإطار القانوني على المرسوم بقانون اتحادي رقم 25 لسنة 2021 بشأن حماية البيانات الشخصية، وهناك التشريعات المتعلّقة بالجرائم الإلكترونية، فضلاً عن السياسات والاستراتيجيات الحكومية بهذا الشأن. تكمن المسؤولية عن الأضرار إذا ما حصل هناك خرقٌ لقواعد حماية البيانات أو الخصوصيَّة من الفِعل الضَّار، أو الإخلال بالالتزام القانوني أو التَّعاقدي المُتعلَّق به. يُشكِّل الإطار الإماراتي منظومةً مُتدرجة لحماية البيانات والخصوصيَّة، لكنَّه لا يزال يواجه مسائل مُتعلّقة بالمسؤولية. [2]

يهدف المرسوم أعلاه إلى حماية سريَّة المعلومات، وخصوصية الأفراد، ووضع إطار لحوكمة البيانات، وتحديد حقوق والتزامات الأطراف المعنيَّة؛ ويتم تطبيقه على معالجة البيانات الشخصيَّة والمُعالجة الإلكترونية وفق شُروط ونطاق القانون، كما يضع قواعد تتعلَّق بمشروعية المُعالجة وموافقة صاحب البيانات، قد تكون مسؤولية هذا المرسوم هي المادة الأوليَّة الَّتي يُبنى عليها القرار الخوارزمي، وبأنَّ جمع أو مُعالجة أو مُشاركة غير مشروعة تكون مصدراً مُستقلاً للمسؤوليَّة. [3]

تُمثِّل الضَّوابط بالنسبة للذكاء الاصطناعي أساساً لمُعالجة البيانات على مبادئ المشروعيَّة والشفافيَّة، وتحديد الغرض وتفعيل البيانات والدَّقة والتَّحديث، واتخاذ القرار المُناسب /التَّدابير وحماية المعلومات من الاختراق. [4] سوف يتم البحث في هذا الفصل في موضوعين، الأول: مفهوم طبيعة المعلومات والضرر الناشئ عنها، الثاني: الأضرار الناشئة عن المخرجات الخوارزمية.

المبحث الأول: مفهوم طبيعة المعلومات والضرر الناشئ عنها

تُعد البيانات والمعلومات هي المادَّة الأولية الَّتي تعمل بها الذكاء الاصطناعي، أمَّا طبيعتها القانونية فتُعد مُدخلاً ضرورياً لتحديد المسؤولية عن الأضرار الَّتي يمكن أن تنشئ عنها، لا تؤدي البيانات وظيفةً تقنيَّة فحسب، إنَّما قد يندرج نوعها كمعلوماتٍ شخصيَّة، أو مهنيَّة، أو ماليَّة، أو صحيَّة، أو اجتماعية. وقد تكون مُتعلّقة بشخصٍ مُحدَّد، أو تتضمَّن معلومات منشورة سابقاً أو يضعها المُستخدم في النظام. أمَّا أهميَّتها فتُصبح عند استخدامها في تدريب النَّموذج، أو في إنتاج المُخرجات. كما أنَّ الذكاء الاصطناعي التوليدي يعتمد على كميَّاتٍ ضخمة من البيانات، وهذه النماذج قد تُثير مُشكلات خاصَّة تتعلَّق بدقَّة المعلومات الَّتي تُنتجها، وبإمكانيَّة حِفظها أو إعادة إنتاجها. [5]

أمَّا من ناحية المعلومة نفسها، فإنَّه يجدر التَّمييز بين المعلومة الَّتي يُقدّمها الفرد للنَّظام وبين البيانات الشخصيَّة الَّتي لها حماية مُستقلة، تتعامل اللائحة GDPR مع البيانات الشخصية باعتبارها محوراً مُستقلاً للحماية، ولها مبادئ تحكم كيفية جمعها ومُعالجتها واستخدامها، مع مُراعاة الشفافيَّة والمشروعيَّة والإنصاف وتحديد الغرض، وتقليل البيانات والدَّقة وسلامة المُعالجة والمُساءلة. ممَّا يستوجب مُراعاة مبدأ الدَّقة في نقل المعلومات، إلَّا إنَّ هذا الأخير يواجه تحدِّيَاً خاصاً مع الذكاء الاصطناعي

[1]- Fernández Llorca, David, Vicky Charisi, Ronan Hamon, Ignacio Sánchez, and Emilia Gómez, "Liability Regimes in the Age of AI: A Use-Case Driven Analysis of the Burden of Proof," Journal of Artificial Intelligence Research, Vol. 76, 2023, pp. 613–644, from the website below: https://doi.org/10.1613/jair.1.14565

[2]- الشامسي، ريم غريب، (2022). حماية الخصوصية الرقمية في ظل تطبيقات الذكاء الاصطناعي: دراسة تحليلية مقارنة، رسالة ماجستير في القانون الخاص، كلية القانون، جامعة الإمارات العربية المتحدة، الإمارات العربية المتحدة، ص15.

[3]- United Arab Emirates, Federal Decree-Law No. (45) Of 2021 Concerning the Protection of Personal Data, Articles 1–5, Official Legislation Portal of the United Arab Emirates, 2021.

[4]- Almaazmi, Nada Mohamed, "Processing Personal Data Without the Data Subject's Consent in Light of Federal Decree-Law No. 45 of 2021," UAEU Law Journal, Vol. 40, No. 1, 2026, pp. 106–138, from the website below: https://doi.org/10.65088/2026.40.1.3

[5]- Novelli, Claudio, Federico Casolari, Philipp Hacker, Giorgio Spedicato, and Luciano Floridi, "Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity," Computer Law & Security Review, Vol. 55, November 2024, Article 106066, https://doi.org/10.1016/j.clsr.2024.106066

بسبب الطبيعة الاحتمالية للمُخرجات، وإمكانية إنتاج معلومات غير دقيقة أو غير مُطابقة لمصدرها المباشر.[1]

وبالحديث عن الضَّرر فإنَّه يتوجَّب معرفة أثرها القانوني، إذ قد ينشأ الضَّرر قبل أن ينتج النَّظام أي مخرج، وقد يكون مصدره البيانات ذاتها، إذا كانت مُضلِّلة أو مشروعة أو مُتحيِّزة، وقد يكون خلال فترة المُعالجة أو في المُخرجات الَّتي يُقدّمها النظام. لذلك، لا ينبغي أن تُبنى المسؤولية على هذا الأخير وحده، حيث إنَّ تعدُّد مصدر الخطأ يتطلَّب تتبُع سلسلةٍ تقنيَّة وقانونية مُتعدِّدة المراحل؛ وبالنسبة لشروط المسؤولية فهناك صعوبة في تحديد الفاعل وإثبات السببيَّة، حيث إنَّ تعدُّد الأطراف المشاركة وتعقيد آلية إنتاج المُخرجات جميعها مُرتبطة بها.[2]

قد يلحق الضَّرر بالمُستخدم نفسه، أي الشخص الذي يتصفَّح النَّظام أو يستعمله، أو عندما يعتمد على معلومةٍ غير صحيحة أو ناقصة، أو مُضلِّلة يُنتجها النظام. قد يتضرَّر المُستخدم مالياً أو مهنياً أو صحيَّاً نتيجة اعتماده على مخرج خوارزمي غير صحيح. أمَّا الغير فيتضرَّر من محتوى يصفه النَّظام بصورةٍ خاطئة، فيكون الضرر من محتوى يصفه النظام بصورةٍ خاطئة أو مُسيئة. وعليه، ينبغي التَّمييز بين الفرد مُتلقّي المعلومة أو الفرد موضوع المعلومة، فيكون الأول قد أنشأ الضَّرر عندما أعاد نشر مخرج النَّظام مع عِلمه بعدم صحّته، أمَّا الآخر فيتضرَّر من التَّشهير والمعلومات غير الصحيحة بحقه. وهذا الأمر كذلك يجعل المسؤولية في هذا الصدد أكثر تعقيداً، إذا ما تمَّ الأخذ بأسبابها بطريقةٍ تقليدية.[3]

وإذا تمَّت الإشارة إلى الاتحاد الأوروبي لناحية ما تمَّ تناوله التَّشريع بشأن الضَّرر، فإنَّ هذا الأخير إذا كان ناشئاً عن المعلومات الشخصيَّة، فإنَّ ذلك يقتضي العودة للائحة GDPR إذا كانت المعالجة بشأن البيانات الشخصيَّة. وقد وضع النظام الأوروبي مجموعة من المبادئ الَّتي تحُد من إمكانية استعمالها بصورةٍ تضُر بصاحبها، لذلك ينبغي توخّي الدَّقة واتخاذ التَّدابير المُناسبة لتصحيحها أو حذفها وفقاً للقواعد المُقرَّرة. أمَّا المشكلة الأكبر فتكون إذا أنتج النَّظام معلوماتٍ خاطئة عن شخصٍ حقيقي، فقد تتحوَّل حالة "هلوسة" النظام إلى معلومةٍ شخصية غير صحيحة، إذا ارتبطت بشخصٍ مُعيَّن أو قابل للتَّعيين. فتدخل فيها حقوق مُعيَّنة منها: الحق في التَّصحيح أو الاعتراض، أو محو البيانات، هذا بالإضافة إلى الحق في التَّعويض عن الضَّرر.[4]

يفرض النظام عالي المخاطر مُتطلبات تتعلَّق بإدارة البيانات وجودتها، مع التَّوثيق والشفافيَّة والرَّقابة البشريَّة والدَّقة، ويجب ألَّا تتعامل هذه البيانات باعتبارها مدخلاً مُحايداً، إنَّما باعتبارها أحد مصادر المخاطر الَّتي يجب إدارتها أساساً مُهماً عند تحديد المسؤولية عن الضَّرر اللَّاحق بالمُستخدم أو الغير.

أمَّا مسألة التَّشهير فتظهر عندما ينتج الذكاء الاصطناعي معلومات كاذبة عن شخصٍ حقيقي بصياغةٍ تبدو واقعية، وإذا كانت المعلومة تمُسّ سمعة شخصٍ مُعيَّن، فإنَّها قد تتحوَّل إلى ضررٍ يمُس أحد حقوقه الشخصيَّة. يتبيَّن أنَّ قواعد التَّشهير التَّقليدية لا تزال قابلة للتطبيق على المحتوى، وعليه يتوجَّب تحديد الأدوار البشريَّة والمؤسسيَّة في إنتاجها ونشرها وإعادة نشرها، وبالأخص دور مُطوِّر النَّظام والجِهة المُشغِّلة وأيضاً المُستخدم الذي يُعيد النَّشر.[5]

وبالنسبة لانتهاك الخصوصيَّة فتُعد إحدى صور الضَّرر، حيث يتمثَّل هذا الأخير في كشف معلوماتٍ شخصيَّة صحيحة دون سندٍ مشروع، أو معالجة بياناتٍ حسَّاسة غير مشروعة، وتسبُب نماذج الذكاء الاصطناعي بهذه الأضرار بسبب تخزينها أو حِفظها لأنماط من بيانات التَّدريب، أو نتيجة إدخال المُستخدم بيانات شخصيَّة عن الطلبات الموجَّهة للنَّظام. تكون جُل المخاطر في مواضع حِفظ البيانات، هجمات استنتاج البيانات، أو العبث بالبيانات الموجودة عبر إدخال بياناتٍ شخصيَّة، أو تسريب

[1]- Novelli, Claudio, Federico Casolari, Philipp Hacker, Giorgio Spedicato, and Luciano Floridi, "Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity," pp: 6-8. Ibid.
[2]- Abouhaiba, Nagwa, Saed Ahmed Khouli, and Maya Khater, "Towards Protecting the Injured Party from Errors and Hallucinations of Artificial Intelligence: A Contemporary Legal Perspective," F1000Research, Vol. 15, 2026, Article 569, from the website below: https://doi.org/10.12688/f1000research.179603.1
[3]- Garfield Tenzer, Leslie Y., "Defamation in the Age of Artificial Intelligence," New York University Annual Survey of American Law, Vol. 80, No. 2, 2024, pp. 135–177.
[4]- Novelli, Claudio, Federico Casolari, Philipp Hacker, Giorgio Spedicato, and Luciano Floridi, "Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity," Ibid.
[5]- Garfield Tenzer, Leslie Y., "Defamation in the Age of Artificial Intelligence," New York University Annual Survey of American Law, Vol. 80, No. 2, 2024, pp. 135–177.

المعلومات الشخصيَّة عبر المُخرجات.[1]

أمَّا في الإمارات العربية المتحدة، فإنَّ القانون يُقرِّر ضوابط لمُعالجة البيانات، ويجعل الأصل أن تخضع المعالجة للشروط القانونية المُقرَّرة مع تنظيم الحالات التي يجوز فيها إجراء المعالجة دون موافقة صاحب البيانات، إلا إنَّ هذا الاستثناء يُثير الحاجة لوضع تنظيمٍ قانوني أكثر تحديداً.[2]

وجاء في المادة (18) من المرسوم حق صاحب البيانات في الاعتراض على القرارات النَّاتجة عن المعالجة الآلية بما فيها التَّوصيف الشخصي، وإذا كان للقرار أثرٌ سلبي عليه. وهذه القاعدة تمنح الشخص المُتأثر بالقرار الخوارزمي أساساً قانونياً للاعتراض كما القانون. وبذلك تكون الحماية في منع الوصول غير المشروع للبيانات، وإلى المعالجة الآلية للبيانات، والأثر الذي تنتجه على المركز القانوني للفرد.

وقد جاء في إحدى الدراسات بأنَّ المسألة القانونية لا تتوقَّف عند حماية البيانات عن التَّسريب، وإنما تمتّد إلى طريقة استخدام البيانات في استخدام قرار، أو إحداث نتيجةٍ تمُس شخص.[3]

ولا يقتصر موضوع التَّشهير والاعتداء على السُمعة والخصوصية على المرسوم الإماراتي، إنَّما يتقاطع العمل به في هذه الجرائم مع التشريعات الجزائية والإلكترونية والقواعد العامة لحماية الحقوق الشخصية. وإنَّ استخدام تقنيات الذكاء الاصطناعي أدَّى إلى ظهور صورٍ جديدة من الجرائم المُرتبطة بالخصوصيَّة. ولكن الصعوبة إذا ما حصل تزييف، فإنَّ هذا الأمر يُشير إلى انتهاك الخصوصيَّة والتَّشهير، ممَّا يعني أنَّه هناك حاجة لتعزيز الحماية القانونية والتعاون الدولي وتحديد المسؤوليات المُرتبطة بها.

المبحث الثاني: الأضرار الناشئة على المخرجات الخوارزمية

إذا كان هناك ضرر نجم عن الذكاء الاصطناعي، فتكون نتيجةً عمليةً لمعالجة البيانات، ولا يقتصر الضَّرر على وقوع خطأ تقني أثناء عملية المعالجة، إنَّما على المُخرجات نفسها التي يكون لها آثار قانونية تؤدي إلى المساس بالحقوق والحريَّات الخاصَّة بالأفراد؛ وهي بطبيعتها تتنوَّع ما بين معلوماتٍ تُسيئ للسُمعة أو تعرض تمييزاً ضد فرد أو توصية تحريضية، أو قراراً آلياً يؤثر على حياة الفرد أو مركز عمله، أو كشف معلوماتٍ سريَّة أو نشر معلوماتٍ ضارَّة. أمَّا خطورتها إذا تمَّ التعامل معها بشكلٍ مُجرَّد، دون أن تكون موضوعية على الرُّغم من أنَّ الناتج الخوارزمي يتأثر ببياناتٍ عنصريَّة أو انحيازيَّة نحو توجهٍ مُعيَّن، وبآلية ترتيب المعلومات. فالمسألة بطبيعتها لا تتعلَّق بالخطأ نفسه، إنَّما بتحديد المسؤولية القانونية الَّتي أحدثتها المُخرجات في العالم الخارجي.[4]

أولاً: المعلومات الكاذبة أو غير الدقيقة:

تُشكّل المعلومات الكاذبة ضرراً ناتجاً عن المُخرجات الخوارزمية، وهذا ما يعرف بـ "الهلوسة" حيث يكون هناك قصورٌ في جمع البيانات أو حصل استنتاجات لا تستند إلى مصادر موثوقة، أمَّا آثارها فتعتمد على أنَّ المعلومات الضَّارة يمكن أن تتحوَّل إلى واقعةٍ ضارَّة يستند إليها المُتصفّح ليبني عليها قراراً، أو ليتأكد من معلومةٍ مُعيَّنة. أمَّا صعوبة الموقف تكون إذا ما حصل هناك إعادة تداول لهذه المعلومة بشكلٍ مُتكرّر، بغضّ النَّظر عن محتواها القانوني أو المالي أو الصحي، وهذه المشكلة أصبحت محل اهتمام في الدراسات القانونية المتعلَّقة بالذكاء الاصطناعي، حيث إنَّ النموذج قد يُقدّم المعلومة الخاصَّة بصياغةٍ جازمة توحي بدرجةٍ من اليقين أنها صحيحة، وهي لا تعكس الحقيقة الَّتي أنتجها.

---

[1]- Novelli, Claudio, Federico Casolari, Philipp Hacker, Giorgio Spedicato, and Luciano Floridi, "Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity," Ibid.

[2]- Almaazmi, Nada Mohamed, "Processing Personal Data without the Data Subject's Consent in Light of Federal Decree-Law No. 45 of 2021," Ibid.

[3]- Chemlali, Laroussi, "La prise de décision automatisée : Une analyse comparative entre le RGPD européen et le Décret-loi fédéral émirati n° 45 de 2021," University of Sharjah Journal of Legal Sciences, Vol. 23, No. 1, 2026, pp. 828–861, from the website below: https://doi.org/10.36394/jls.v23.i1.28

[4]- Lidsky, Lyrissa Barnett, and Andrew Daves, "Inevitable Errors: Defamation by Hallucination in AI Reasoning Models," Journal of Free Speech Law, Vol. 6, 2025, pp. 477–561.

وإذا كانت هذه المعلومات تتعلَّق ببيانات الشخص أو مؤهلاته، فإنَّها قد تؤثر في سُمعة أو فُرصه في العمل أو حصوله على خدمة. ومن حيث المسؤولية فإنَّه ينبغي البحث في الجهة الَّتي قامت بتشغيله أو إتاحته، ومدى إمكانية توقُّع الخطأ، والبحث في مسؤولية المستخدم الذي يُعيد نشر المعلومات الكاذبة، مع علمه بعدم موثوقيتها أو دون إسنادها إلى المرجع الذي أصدرها. [1]

ثانياً: التشهير وإيذاء السمعة:

يُعدّ هذا النوع من الأضرار هو أكثرها وضوحاً، إذ إن نشرها يؤدي إلى التَّقليل من سُمعة الفرد، أو التَّضليل أو الإيهام أو الكذب وغيرها من الأمور الَّلاحقة بالسمعة. أمَّا السوء الذي يطال هذا الفرد فيكون إذا تعامل المُتصفّح مع المعلومات الَّتي قدَّمتها المُخرجات الخوارزمية، على أنها معلومات حقيقية وتمَّ تداولها ونشرها للغير، ممَّا يجعل تحديد الفاعل الذي جمع هذه المعلومات أكثر تعقيداً. وقد تبيَّن أنَّ الذكاء الاصطناعي لا يلغي القواعد التقليديَّة للمسؤولية عن التَّشهير، إنَّما يؤدي إلى إثارة أسئلة تتعلَّق بتوزيع المسؤولية بين مُطوّر النَّظام ومُشغّله، والمُستخدم والجِهات الَّتي بإمكانها منع الضَّرر. [2]

تجدر الإشارة بأنَّ المعلومات إذا بقيت بين المُتصفّح والنَّظام، فإنَّها قد تختلف قانوناً، حيث إنَّه إذا قام المُتصفّح بنقلها من مكانة الاستخدام الخاص لينشرها وتصبح أمام التداول العام؛ فإنَّ الضَّرر بهذه الحالة يتوسَّع بصورةٍ أكبر، ويثير مسألة البحث في مسؤولية المستخدم الذي ينشر المُخرجات التَّشهيرية أو الاحتفاظ بالسّجلات الَّلازمة لإثبات كيفية إنتاج المخرج. [3]

ثالثاً: التمييز والتحيز الخوارزمي والتحريض:

عندما يقوم المُتصفّح بطلب معلوماتٍ مُعيَّنة، قد تكون المُخرجات الخوارزمية النَّاتجة عنها مُستندة إلى معلوماتٍ تعكس تحيُّزات تاريخية أو اجتماعية، أو تصدر معلوماتها بناءً على مُتغيِّرات قد تبدو محايدة بالصورة الأولى إلا إنها مختلفة في جوهرها، حيث تحمل تمييزاً أو تحيُّزاً نحو فكرةٍ أو هدفٍ مُعيَّن. أمَّا من الناحية القانونية، فإنَّه لا يشترط في المُخرجات الخوارزمية ورود عبارة تمييزيَّة صريحة، حيث يكون التَّمييز غير مباشر، ولكن هذا الأمر قد يؤدي إلى تحميل فئةٍ مُعيَّنة عبئاً أو حِرمانها من فُرصة أو خِدمةٍ بصورةٍ غير جيدة. [4]

قد يخرج النظام نتائج تمييزية، حتى عندما لا يكون المُتغيِّر المحمي مُدرجاً صراحةً من ضمن البيانات التي يتم الاعتماد عليها، لأنَّها قد تكون مُرتبطة به بصورةٍ غير مباشرة. حيث إنَّ تقييم مشروعية هذا المخرج يقوم على فحص البيانات المُستخدمة، وطريقة بناء النموذج والمُتغيِّرات الدَّاخلة إلى القرار، والنتائج الفعليَّة دون الاقتصار على حياد الصياغة البرمجيَّة. [5]

أمَّا بشأن التَّحريض أو التَّشجيع أو المساعدة على ارتكاب فعلٍ ضار، فإنَّ الضَّرر يكمن إذا ما كان المحتوى موجَّه إلى أشخاصٍ أو جماعاتٍ مُحدَّدة، أو إذا تضمَّنت المُخرجات توصيةً بزيادة ظهور مُحتوى ضار نتيجة آليات التفاعل والتَّخصيص. حيث إنَّ التَّضليل في هذه الحالة يشمل آليات توزيعها وتضخيم انتشارها، ممَّا يؤدي إلى أضرار تمُسّ الأمن والصحَّة والحقوق. [6]

رابعاً: القرارات الآلية وإفشاء السر الوظيفي:

برز لدى البعض الاعتماد الجوهري على الذكاء الاصطناعي في كافَّة المجالات، حتى وصل الأمر إلى العلاقات الأسرية واتخاذ القرارات فيها، وكيفيَّة حلّ مشكلاتها من غير التطرُّق المُفصَّل للوقائع، الأمر الذي أحدث تغييرات في مجرى القرار

1- Lidsky, Lyrissa Barnett, and Andrew Daves, "Inevitable Errors: Defamation by Hallucination in AI Reasoning Models," Ibid. pp. 514 – 525.
2- Lidsky, Lyrissa Barnett, and Andrew Daves, "Inevitable Errors: Defamation by Hallucination in AI Reasoning Models," Ibid. pp. 514 – 525.
3- Ernst Karner, Bernhard A. Koch, and Mark A. Geistfeld, Comparative Law Study on Civil Liability for Artificial Intelligence, Ibid, p: 9 -17.
4- Xenidis, Raphaële, "Tuning EU Equality Law to Algorithmic Discrimination: Three Pathways to Resilience," Maastricht Journal of European and Comparative Law, Vol. 27, No. 6, 2020, pp. 736–758, from the website below: https://doi.org/10.1177/1023263X20982173
5- Arnold, David, Will Dobbie, and Peter Hull, "Measuring Racial Discrimination in Algorithms," AEA Papers and Proceedings, Vol. 111, May 2021, pp. 49–54, from the website below: https://doi.org/10.1257/pandp.20211080
6- Sun, Haochen, "Regulating Algorithmic Disinformation," Columbia Journal of Law & the Arts, Vol. 46, No. 4, 2023, pp. 367–417, from the website below: https://doi.org/10.52214/jla.v46i3.11237

دون تحديد مدى ايجابياته أو سلبياته وأثره على واقع الأسرة. يزداد الأمر سوءاً إذا كان القرار الآلي المُتَّخذ ذات تأثير على المركز القانوني أو الاقتصادي أو الاجتماعي. جاء في اللائحة العامة لحماية البيانات GDPR المادة (22) منها ما أولى هذه الأهمية، إذ نصَّت على حق الشخص في ألَّا يخضع لقرارٍ قائم حصراً على المعالجة الآلية، إذا كان ينتج أثاراً قانونية، أو يؤثر فيه تأثيراً مُماثلاً بصورةٍ جوهريَّة مع وجود استثناءاتٍ وضماناتٍ مُحدَّدة. [1]

ومؤدى ذلك قد تتقلَّص قُدرة الفرد على معرفة الأساس الذي بُني عليه الاعتراض، أو جرى الاعتراض عليه، أو طلب التَّدخل البشري الحقيقي. لذلك يفترض بالقرار الآلي أن يكون مُرتبطاً بمبادئ الشفافيَّة والمُساءلة وقابليته للطَّعن. أمَّا غموض الخوارزمية أو ما يُعرف بـ "الصندوق الأسود" فإنَّه قد يجعل اكتشاف الخطأ أو التَّمييز أمراً صعباً، ما يبرر أهمية الحق في الوصول إلى المعلومات، وأيضاً التَّفسير والتدخُّل البشري والطعن في القرار. [2]

أمَّا بالنسبة لإفشاء السرّ الوظيفي، فيكون عندما يقوم الموظف بإدخال معلوماتٍ سريَّة إلى نظام الذكاء الاصطناعي لغرض تحليلها أو صياغة مستندات أو معلومات ذات صلة، أو اتخاذ معالجة لمشكلةٍ مُعيَّنة، بعدها يستخدم نظام الذكاء الاصطناعي هذه المعلومات، ويقوم بإظهار مُخرجاته لمستخدمٍ آخر غير مُخوَّل بالاطلاع عليها، وهذا يشمل المعلومات التجارية، العقود، المعلومات الوظيفية، المُراسلات المهنيَّة، العقود السريَّة؛ كما أنه له الكثير من الآثار السلبيَّة لناحية الشركة في الجهة الأولى، ثم لناحية المستخدم، لأنَّه الفرد الذي أدخل المعلومات بُغية غرضٍ مُعيَّن، فأدى بذلك إلى إفشاء السرّ الوظيفي. [3]

وقد بيَّنت الدراسات الحديثة أنَّ الاستخدام غير المنضبط للذكاء الاصطناعي من قِبل الموظَّفين والمُتعاقدين قد يخلق خطراً على سريَّة المعلومات، لأنَّ البيانات قد تدخل في عمليات مُعالجة، أو تخزين، أو استرجاع، ما يتجاوز الحد الذي قصده صاحب المعلومات. وتكون المسؤولية في هذه الحالة عن فعل الإفشاء ذاته، أو عن الإخلال بواجب الحيطة والرَّقابة على استخدام النِّظام. [4]

أمَّا بشأن نشر المعلومات الضَّارة، فإنَّها تختلف عن إفشاء السّر الوظيفي، حيث يكون الضَّرر في تضاعف نتيجة تداولها وإعادة نشرها وتضخيم وصولها، حيث إنَّ البيئة نفسها تسمح بالانتقال السريع للمعلومات من مستخدمٍ لآخر، وقد تقوم خوارزميات بوضع توصية بظهورها وفق أولويَّةٍ مُعيَّنة بسبب الجذب والتفاعل الذي يجري عليها، ويكون في بعض الأحيان المخرج نفسه ضاراً، لكنَّ آلية نشره قد تحوَّل الضَّرر الفردي إلى جماعي؛ فالتَّضخيم في هذه المرحلة لا يكتفي أحياناً بالمُحتوى المُضلِّل إنَّما يبني عليه، ويُساهم في انتشاره بشكلٍ أوسع. [5]

وحتى يتم تحديد المسؤولية عن هذا الفعل، فإنَّه ينبغي تحديد الفعل الذي قام به كُل طرف، ومدى العِلم بطبيعة المحتوى ومدى إمكانية توقُّع الضَّرر، وإذا كان هناك نص قانوني يمنع ذلك، وكذلك مدى مساهمة كُل طرف في توقع النتيجة الضارة، وعليه ينتقل موضع المسؤولية من مُجرد إنتاج آلي، إلى فِعلٍ بشري مُستقل يساهم في النَّشر والاعتماد أو الاستخدام ضدَّ الغير. [6]

وسوف ونبحث في الفصل الثاني عن المسؤولية المدنية والجنائية والإدارية عن أضرار الذكاء الاصطناعي بين كلٍ من الاتحاد

---

[1]- Bygrave, Lee A., "Article 22: Automated Individual Decision-Making, Including Profiling," in Christopher Kuner, Lee A. Bygrave, and Christopher Docksey (eds.), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press, Oxford, 2020, pp. 522–542.

[2]- Bygrave, Lee A., "Article 22: Automated Individual Decision-Making, Including Profiling," Ibid.

[3]- Aboelazm, Karem Sayed, Khalid Mohamed Dganni, Sumaya Aljahoori, and Zahid Hussain, "ChatGPT and the Erosion of Confidentiality: Legal and Ethical Implications of Generative AI Use in Public Office," International Journal of Law and Management, 2026, pp. 1–26, from the website below: https://doi.org/10.1108/IJLMA-02-2026-0097.

[4]- Lee, Kyung-Min, "A Study on the Use of Generative AI and Protection of Trade Secrets," Legal Theory & Practice Review, Vol. 12, No. 4, 2024, pp. 205–217, from the website below: https://doi.org/10.30833/LTPR.2024.11.12.4.205.

[5]- Chesterman, Simon, "Lawful but Awful: Evolving Legislative Responses to Address Online Misinformation, Disinformation, and Mal-Information in the Age of Generative AI," The American Journal of Comparative Law, Vol. 72, No. 4, 2024, pp. 933–965, from the website below: https://doi.org/10.1093/ajcl/avaf020.

[6]- Lee, Kyung-Min, "A Study on the Use of Generative AI and Protection of Trade Secrets," Ibid.

الأوروبي والإمارات العربية المتحدة.

الفصل الثاني: المسؤولية المدنية والجنائية والإدارية عن أضرار الذكاء الاصطناعي مقارنة بين الاتحاد الأوربي والإمارات العربية المتحدة

إنَّ اعتماد الفرد في الآونة الأخيرة على الذكاء الاصطناعي في مُختلف الجوانب سواء أكانت قانونية، اجتماعية، اقتصادية، وحتى شخصيَّة بالإرادة الفردية، ونتيجة التطوّر المُستمر، وسهولة الوصول إلى المعلومات المُرتبطة بالأنظمة الخوارزمية المساعدة، الَّتي تؤدي على إنتاج كمياتٍ كبيرة من البيانات المتنوّعة وإصدار التَّوصيات، وفي بعض الأحيان اتخاذ القرارات بشكلٍ مُباشر أو غير مُباشر، باعتمادٍ تام أو شِبه تام على الذكاء الاصطناعي، وقد أوجد ذلك مخاطر قانونية عن المُخرجات بسبب قُدرتها على احتمال حُدوث ضرر، أو تناقُل أخطاء من شأنها إلحاق أضرار ماديَّة أو معنويَّة، سواء أكانت تقع على الأفراد أو المؤسَّسات أو إلحاق الضَّرر نفسه بالمصلحة العامَّة أو الغير. ففي هذا النظام تتعدَّد الأطراف المُشاركة بدءاً من التَّصميم والتَّطوير، التَّدريب، إخراج البيانات وتشغيلها، وحتَّى استخدامها وجميع ما ذكر. يفرض إعادة النَّظر في مدى كفاية قواعد المسؤولية لاسيَّما فيما يتعلَّق بإثبات الخطأ والضَّرر، والعلاقة السببيَّة الذي يمكن إسناد الضَّرر إليه. [1]

أمَّا المشكلة في هذه الحالة فتكمن في معرفة من يتحمَّل الضَّرر الناشئ عن هذه التقنيَّة، وفي حدود أي نظام من أنظمة المسؤولية، فقد يكون في الواقعة الواحدة التالي: مُطوّر النّظام، مُزوّد البيانات، المُنتج او المُورّد، الجهة المُشغِلة والمُستخدم النهائي. حيث يجب ربط الجهة الإدارية بتلك التي اعتمدت على المُخرجات الخوارزمية باتخاذ قرارٍ يمُس أحد الأفراد. وقد تبيَّن أنَّ تعدُّد المُتدخلين في دورة حياة النَّظام، يثير مُشكلة تعدُّد الأيادي حيث يصعب تحديد الفاعل الذي تسبَّب بصورةٍ مُباشرة، وبالتالي تحديد مسؤوليته.

وعليه، يتكون هذا الفصل من ثلاثة مباحث، الأول: المسؤولية المدنية والتعويض عن أضرار الذكاء الاصطناعي، الثاني: المسؤولية الإدارية والجزاءات والرقابة، والثالث عن المسؤولية الجنائية وإسناد الجريمة.

المبحث الأول: المسؤولية المدنية والتعويض عن أضرار الذكاء الاصطناعي

تتمثَّل المخاطر القانونية النَّاتجة عن الذكاء الاصطناعي بهذه الحالة بأنَّها ليست تقنيَّة فحسب، إنَّما نتاجاً بشريَّاً قد يؤدي إلى إنتاج معلوماتٍ غير صحيحة، أو اتخاذ قرار تمييزي، أو معالجة بيانات شخصيَّة بصورةٍ غير مشروعة، أو تقديم توصية من شأنها إحداث ضرراً جسدياً أو مالياً أو معنويَّاً مُتعلّق بالسُمعة. أمَّا الصعوبة فتكمن في معرفة الفاعل في كُل هذا الضَّرر ونسب العلاقة السببيَّة. إلَّا إنَّ الخصائص المعتمدة من الذكاء الاصطناعي المُتمثّلة بالاستقلالية والتَّعقيد، والقُدرة على التَّعلُم والتَّكيُف وصُعوبة تفسير النَّتائج هي الَّتي تحكُم الموقف. [2]

اتَّجه الاتحاد الأوروبي إلى بناء منظومةٍ تشريعيَّة مُتعدَّدة المستويات، التي تجمع بين السلامة والوقاية وحماية البيانات الشخصية في الَّلائحة العامة، والمسؤولية عن المنتجات المَعِيبة كما جاء في التوجيه الجديد رقم 2024/2853 مع وضع قواعد المسؤولية الوطنية.

في حين أنَّ الإمارات العربية المتحدة وحتَّى تاريخه، فإنَّه لا يوجد فيها قانون اتحادي شامل مُستقل للمسؤولية المدنيَّة، إنَّما تعتمد بصورةٍ موسَّعة على القواعد العامَّة في قانون المعاملات المدنية الجديد، قانون حماية البيانات الشخصية، قانون مكافحة الشائعات والجرائم الإلكترونية والتَّشريعات القطاعية المُتَّصلة بها.

وجاء في دراسةٍ إماراتية بهذا الشأن أنَّ القواعد العامَّة يُمكن أن تستوعب جانباً من أضرار الذكاء الاصطناعي، لكن في المقابل هناك صعوبة في إثبات الخطأ والعلاقة السببيَّة وفي تحديد المسؤول عن الضَّرر. [3]

---

[1]- Zech, Herbert, "Liability for AI: Public Policy Considerations," ERA Forum, Vol. 22, No. 1, 2021, pp. 147–158, from the website below: https://doi.org/10.1007/s12027-020-00648-0

[2]- Zech, Herbert, "Liability for AI: Public Policy Considerations," Ibid.

[3]- النقبي، محمد سالم، وعثمان، أيمن. (2024). المسؤولية المدنية الناشئة عن أضرار تطبيقات الذكاء الاصطناعي في مهنة أعمال المحاماة: دراسة مقارنة بين القانون الإماراتي والأوروبي، مجلة جامعة الشارقة للعلوم القانونية، مجلد 21، العدد 4، ص 225 – 255.

أولاً: في الاتحاد الأوروبي:

أوجد قانون الذكاء الاصطناعي AI Act الذي وضع قواعد موحَّدة بشأن تطوير أنظمة الذكاء الاصطناعي ووضعها في السوق، واستخدامها على أساس تصنيف المخاطر مُتضمناً التزامات خاصَّة على الأنظمة عالية الخطورة، تكون الالتزامات مُتعلِّقة بالسلامة وإدارة المخاطر والتَّوثيق والرَّقابة البشريَّة الَّتي لها أثر غير مُباشر في دعاوى المسؤولية المدنيَة. حيث منح القانون الحق للشخص المُتأثر في تقديم شكوى إلى سُلطة مُراقبة السوق، وعلى الحق في تفسير واضح وذات معنى في بعض القرارات الصادرة بناءً على المُخرجات عالية الخطورة. [1]

أمَّا بالنسبة للتَّعويض فإنَّ الإثبات يكون في حال مُخالفة الالتزامات القانونيَّة المُتعلِّقة بالسلامة أو التوثيق أو الرقابة البشريَّة، ومن شأن هذا الإثبات أن يساعد المُتضرِّر في تحديد وجود خللٍ أو الإخلال بواجبٍ قانوني. حيث إنَّ قواعد المسؤولية تتمثَّل في السلامة التَّنظيمية التي قد تصبح مِعياراً مُهمَّاً لتقييم العيب في المُنتج أو الإخلال بواجب العناية. [2]

وليعالج القانون أيضاً مشكلة عدم تماثُل المعلومات بين المُتضرّر والمُنتج التَّقني، إذ جاء في المادة (9) الإفصاح عن الأدلَّة، والمادة (10) قواعد عبء الإثبات وافتراض العيب، أو السببيَّة في بعض الحالات، حيث إنَّ المُتضرِّر قد يستطيع إثبات النَّتيجة الضَّارة دون إمكانية الوصول إلى الرابط أو البيانات اللَّازمة، أو سجلات التَّشغيل الَّتي تُفسّر كيفية وقوع الخطأ.

تكون مسؤولية مُطوِّر الذكاء الاصطناعي أو المُنتج وفق القواعد الخاصَّة بالمُنتجات المعيبة أو القواعد الوطنية للمسؤولية عن الخطأ، إذا كان الضَّرر ناتجاً عن عيب في تصميم النِّظام أو خلل في البَّرمجيات، أو عدم استيفاء مُتطلبات السلامة أو مُعالجة الخطر المُتوقَّع. حيث إنَّ التوجيه 2024/2853 لم يحصر الأشياء المادية بل تكيَّف مع المُنتجات الرَّقمية. [3]

أمَّا مسؤولية مُزوِّد النِّظام ومُشغِّله، فتكون عند استخدامه خارج الغرض المُتوَّقع أو عبر تجاهل تحذيراته أو عدم الرَّقابة رغم وجود شرط الالتزام بالرَّقابة، عندها تتوزَّع المسؤولية، أو تنتقل وفقاً للقواعد الوطنية أو التعاقدية المعمول بها. أمَّا أهميَّته فتكون في مدى السيطرة على الخطر، حيث إنَّ التَّبعات تتمثَّل في مدى الإخفاق في اتخاذ الاحتياطات.

ومن ناحية مسؤولية المُتحكّم أو مُعالج البيانات فترتبط بالبيانات الشخصيَّة، حيث وضعت اللائحة GDPR في المادة (82) منها الحق لكل شخص لحِقَ به ضررٌ مادي أو غير مادي في الحُصول على تعويض من المُتحكّم أو المُعالج. يكون المُتحكّم مسؤول عن الضَّرر النَّاجم عن مُعالجة تخالف ما نصَّت عليه اللائحة؛ أمَّا المُعالج فتكون مسؤوليته إذا تصرَّف خارج تعليمات المُتحكَّم، ويتحمَّل كُلاً منهما المسؤولية عن كامل الضَّرر تجاه صاحب البيانات ودفع التَّعويض كاملاً، أو الرجوع على نصيب كُلاً منهم بالمسؤولية. وتكون هذه الأخيرة بصرف النَّظر عن تلك المفروضة في القانون المدني الوطني.

قضت محكمة العدل الأوروبي في القضية OQ v Land Hessen /SCHUFA Holding AG, C-634/21 إذ قرَّرت في قرارها الصَّادر بتاريخ 2023/12/7 أن إنشاء جهة مُختصَّة بالمعلومات الائتمانية لقيمة احتمالية لآلية تتعلَّق بقُدرة الشَّخص على الوفاء بالتزاماته المستقبلية بعد اتخاذ (قرارٍ فردي آلي) عندما يعتمد طرف ثالث بصورةٍ قويَّة على هذه القيمة، في إنشاء علاقةٍ تعاقدية مع الشخص أو تنفيذها أو إنهائها. أمَّا أهمية الحُكم فتكمن في منع التحايل على القرار الآلي، بمجرد القول أنَّ الخوارزمية لم تصدر القرار النهائي بنفسها، إنما وضعت توصية اعتمدت عليها الجهة البشريَّة في إصدار قرارها النهائي.

ثانياً: في الإمارات العربية المتحدة:

بالعودة إلى القوانين المعمول بها في الإمارات والمذكورة أعلاه، فإنَّ قانون المعاملات المدنية الجديد رقم 25 لسنة 2025 الذي ألغى العمل بالقانون السابق رقم 5 لسنة 1985، أقرَّ باب الفعل الضَّار في المادة (245) على مبدأ التَّعويض عن الضَّرر،

[1]- European Parliament and Council of the European Union, Regulation (EU) 2024/1689 of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), Ibid.

[2]- Mayrhofer, Ann-Kristin, "AI Act and New Product Liability Directive: The Interplay between AI Safety Regulation and Compensation," Cambridge Forum on AI: Law and Governance, Vol. 2, 2026, Article e13, pp. 1–20, from the website below: https://doi.org/10.1017/cfl.2026.10048.

[3]- Fossati, Curzio, "AI Systems and Product Liability in the EU: A Private International Law Analysis," EU and Comparative Law Issues and Challenges Series (ECLIC), Vol. 9, 2025, pp. 545–563, from the website below: https://doi.org/10.25234/eclic/38130.

والمادة (255) المتعلِّقة بتقدير التعويض الذي يكون بمِقدار الخسارة الَّتي لحقت بالمُتضرر وما فاته من كسب متى كان ذلك نتيجة طبيعية للفِعل الضَّار، مع الحق بالتَّعويض النقدي كما تُجيزه المحكمة (المادة 256) والحكم بإعادة الحال إلى ما كان عليه.

وعليه يُمكن إدخال الضَّرر الخوارزمي ضمن إطار الفِعل الضَّار، متى أمكن إثبات الضَّرر والفِعل والعلاقة السببيَّة، ونِسبة ذلك إلى الفاعل (المسؤول عنه قانوناً).

تقع المسؤولية على مُطوَّر النِّظام إذا ثبت أنَّ الضرر يعود إلى خطأ في التَّصميم أو البرمجة أو الاختبار، ومدى تداخل عوامل أخرى أقرَّت بذلك كطريقة التَّشغيل للنِّظام، أو استخدامه بصورةٍ مُخالفة. أمَّا الصعوبة فتكون في تحديد الشخص الذي يمكن إسناد الضَّرر إليه.

ومن ناحية مسؤولية مُشغِّل النِّظام فتكون مُتحقِّقة عند الحاجة إلى إشرافٍ بشري مُستمر، حيث أهملت الجهة المسؤولة ذلك من ناحية تعليمات الاستخدام أو تجاهلت نتائج غير طبيعية، أو السماح بالاستخدام في غير ما هو مُصمَّم له، ممَّا يحوِّله إلى مصدر خطأ. وتقع المسؤولية إذا ما أدَّى الفعل إلى اتخاذ قراراتٍ تؤثر في خدمة العملاء، أو من غير المحافظة على سلامة البيانات أو النِّظام، فيكون القرار الآلي لا يؤدي إلى مُسائلة النظام كونها الجهة الَّتي اختارته وأدخلته في نشاطها. [1]

أمَّا مسؤولية المُستخدم، فتكون إذا ثبت عِلمه بأنَّ المخرج غير صحيح أو خطير، وقام باعتماده؛ وهذا يُثير حالات التَّشهير والبيانات الكاذبة وتداول المعلومات الضَّارة، ويُعد هذا السبب المُباشر للضَّرر.

وبالعودة إلى قانون حماية البيانات الشخصية رقم 45 لسنة 2021، فقد وضع إطاراً عاماً لمعالجة البيانات وحمايتها وأصبح تطبيقه على المعالجة الَّتي تتم بصورةٍ آلية أو إلكترونية في الحالات الَّتي حدَّدها القانون، وذلك بعد أن دخل حيِّز التنفيذ بتاريخ 2022/1/2. أمَّا أهميَّته فتكمن في العمل على تنظيم المُتحكم في البيانات والمُعالج، ويضع التزامات فيما يتعلَّق بوجوب التَّحقُّق من صحَّة البيانات وسلامتها وأمنها، هذا بالإضافة إلى وضع تقييمات تتعلَّق بالمخاطر، وهذا يظهر من خلال تقييم أثر حماية البيانات، عندما تكون المعالجة عالية المخاطر أو فيها شخصيَّة بصورةٍ غير مشروعة، أو إذا تم استخدام بياناتٍ غير دقيقة، هذا فضلاً عن المسؤولية المدنيَّة التي تُفرض بتحقُّق شُروطها.

ومن ناحية الضَّرر، فقد لا يكون نتيجة عيبٍ مادي، إنَّما بسبب معلومة، أو توصية، أو تصنيف أو قرار نتجه النظام. ويتعامل القانون الإماراتي وفقاً لأحكام المعاملات المدنية الجديد، وقانون حماية البيانات الشخصية، وأيضاً المتعلق بمكافحة الشائعات والجرائم الإلكترونية، وذلك حسب طبيعة الضرر والفعل الذي أدى إليه.

وفيما يتعلَّق بالتَّعويض فإنه يُقدَّر على أساس الخسارة وما فات من ربح، ويُجيز القانون التَّعويض النقدي، ويكون للمحكمة سُلطة إعادة الحال إلى ما كانت عليه، أو الأمر بأداء عملٍ مُعيَّن، وهذا يكون مقابل الضَّرر سواء أكان مادي أو معنوي.

جاء في أحكامٍ صادرة عن المحاكم الإماراتية ما تناول المسؤولية عن الفِعل الضَّار، حيث أورد النصوص المُتعلِّقة بالضَّرر المباشر والضَّرر المُتسبَّب وتعدُّد المسؤولين، مُبيناً كيفية التعامل القضائي مع مبادئ المسؤولية المدنيَّة العامَّة الذي يمكن أن تكون ذات صلة، عندما ينشأ نزاع في المستقبل بشأن النِّظام الذكي. [2]

ومن خلال كِلا النموذجين فهناك اتجاه مشترك في عدم منح الذكاء الاصطناعي شخصيَّة قانونية مُستقلة لتحميله المسؤولية، أمَّا التحدِّي الأكبر فيكون بمدى إمكانية التَّعويض، وفي مدى ضمان قُدرة المُتضرَّر في الحُصول على الأدلَّة التقنيَّة، وإثبات العلاقة السببيَّة والمسؤول عن ذلك، وهذا يتطلَّب إعمال قواعد الشفافيَّة والتَّوثيق، والإفصاح عن المعلومات، وتأمين الأدلَّة وأهميَّة الرَّقابة البشريَّة، وهذا له أهميةً واسعة في بناء نظامٍ فعَّال لهذه المسؤولية.

[1]- النقبي، محمد سالم، وعثمان، أيمن. (2024). المسؤولية المدنية الناشئة عن أضرار تطبيقات الذكاء الاصطناعي في مهنة أعمال المحاماة: دراسة مقارنة بين القانون الإماراتي والأوروبي، المرجع السابق.

[2]- Union Properties PJSC & Anor v Trinkler & Partners Ltd & Others, ADGMCFI 0010 (Court of First Instance, Abu Dhabi Global Market, 6 March 2026.

المبحث الثاني: المسؤولية الإدارية والجزاءات والرقابة

أصبح الذكاء الاصطناعي أداة من أدوات الإدارة الحديثة ووسيلةً لاتخاذ القرارات في بعض الأحيان، هذا بالإضافة إلى إدارة الخدمات العامَّة وتحليل المخاطر. أمَّا المسؤولية في هذه الناحية فتكون في خصوصية مصدر الضَّرر، حيث إنَّ المُخرجات الخوارزمية تُساهم في تكوين القرار أو اتخاذه بصورةٍ آلية، ممَّا يُثير مشكلة تتمثَّل في مدى اتخاذ الإدارة هذا القرار وإسناد الخطأ إليها. والأصل أنَّ المسؤولية تقوم على وجود خطأ أو نشاط إداري غير مشروع، أو حالة من حالات المسؤولية دون خطأ؛ وأنَّ الذكاء الاصطناعي يُغيِّر طبيعة الخطأ، حيث يكون لهذا الأخير دورٌ في اختيارٍ غير مُلائم أو إدخال بياناتٍ غير صحيحة، أو في اعتماد الإدارة على مُخرجات النظام بصورةٍ آلية، دون أن تخضع لمراجعةٍ بشريَّة، أو عندما تستمر الإدارة في تشغيل النَّظام على الرُّغم من المُخرجات الخاطئة أو التَّمييزية. تكون المسؤولية في هذه الحالة عندما تكون الإدارة قد أخطأت في اختيار النَّظام، أو في تصميم طريقة استخدامه، أو وضع أُسُسٍ لِمُراقبته، أو الاعتماد على نتائجه بصورةٍ تامَّة. وبذلك يجب البحث عن الشخص أو الجهة البشرية التي تكون مُلزمة قانوناً بكل ما ورد في وضع الرقابة على النظام. [1]

تقوم المسؤولية لهذه الناحية على صورتين: الأولى هي مسؤولية الإدارة القائمة على الخطأ، والثانية في إمكانية قيام المسؤولية بدون خطأ. وهذا الأمر يكون عندما تستخدم الإدارة نظاماً خوارزمياً في إصدار قرارٍ أو توصية أو معلومة، ثم تثبُت الضَّرر بسبب خللٍ أدَّى لِظُهوره، وكان على الإدارة أن تلتزم بواجبات التَّحقُق والاختبار والرَّقابة مُسبقاً للحؤول دون وقوعه. وفي حال كان ذلك دون خطأ، فيحدث عندما يكون النشاط مشروعاً بحد ذاته، أمَّا استخدامه فيكون عالي الخطورة، ممَّا يؤدي إلى إحداث ضررٍ استثنائي أو غير عادي يستوجب التَّعويض كما هو منصوص عليه قانوناً.

ومن الأضرار الَّتي تحصل في هذه الحالة، عندما يتم اختيار نظام لا يتلاءم مع عمل الإدارة، أو تجاهل التَّدريب المُتمرَّس على أهمية البيانات، عدم متابعة أداء النظام ومُخرجاته، وغيرها من الأمور الَّتي تتطلَّب حداً أدنى من العناية الواجبة قبل صُدور القرار الآلي، وهذا يمتدُ إلى دورة حياة نظامٍ كاملة، تبدأ من الاختيار وتنتهي بالمُراقبة والتَّحديث، وربما الإيقاف في بعض الأحيان. [2]

ويمكن تصوَّر الخطأ في إحدى الحالات: الاختيار، التَّصميم، البيانات، التَّشغيل، الإشراف، الاعتماد على المُخرجات، الخطأ البشري بسبب عدم التَّدخُل، وعدم تصحيح القرار أو وقف النظام بعد بيان الخطأ. فإذا كانت الإدارة تعلم بوجود قُصورٍ في النظام واستمرت في اعتماده، فإنَّ مسؤوليتها تكون قائمة ولو كان أصل الخلل الفني أو التَّقني تابعاً للنظام نفسه. وقد جاء في إحدى الدراسات ذات الصلة أنَّ احتمال إصدار القرار بواسطة الذكاء الاصطناعي، لا يعفي الإدارة من ضمان توافر أركان القرار الإداري، ومن حوكمة الإجراءات التي تسبق إصداره. [3]

أولاً: الرقابة الإدارية:

تُعدّ الرقابة الإدارية واجبة، وتتَّصِف بأنَّها وقائية وتكون بدءاً من إدخال النظام إلى العمل وصولاً إلى التَّتبُع لِمَا بعد وقوع الضَّرر. تتمثَّل أولاً في وضع برمجةٍ مُعيَّنة تُحدَّد طبيعة الضَّرر، ثُم فحص البيانات المُستخدمة، ثم تحديد الأشخاص، تقييم احتمالات الخطأ أو التَّمييز، وضع مستوى الإشراف البشري، ونظام للتَّصحيح أو وقف الاستخدام المُتعثِّر. أمَّا أهمية هذه الرقابة فتكمن في حِفظ الحقوق الأساسية الَّتي قد تمُسّ بالحُريَّة أو السُمعة أو الحُصول على خِدمة؛ وذلك لأنَّ طلب التَّعويض عن الضَّرر قد لا يكون كافياً لإعادة الوضع إلى ما كان عليه. يُعدّ التَّقييم إحدى أهم أدواتها، حيث يقع على الجِهات العامَّة أو الخاصَّة تقييم الخدمات العامَّة قبل نشر نظام عالي الخطورة، حيث يفترض إجراء تقييم لأثره على الحقوق الأساسية. ويشمل ذلك تحديد العمليات التي سيعتمدها النظام وتحديد الفئات التي قد تتأثر به، والمخاطر المُحددة للضَّرر والإجراءات الواجبة

---

[1]- الظهوري، فهد سعيد، والنجيفي، مصطفى سالم مصطفى. (2024) مسؤولية الإدارة عن استخدامات الذكاء الاصطناعي على أساس الخطأ. مجلة جامعة الشارقة للعلوم القانونية، 21(1)، 12.i1.v21.10.36394/jls.https://doi.org/ 329–301.

[2]- Mir, Oriol. (2024). "Algorithms, Automation, and Administrative Procedure at EU Level." In Herwig C. H. Hofmann and Felix Pflücke (eds.), Governance of Automated Decision-Making and EU Law (pp. 52–77). Oxford University Press. From the website below: https://doi.org/10.1093/9780198919575.003.0003.

[3]- الواحدي، عبد الحميد أحمد. (2024) أركان القرار الإداري في عصر الذكاء الاصطناعي. مجلة جامعة الإمارات للبحوث القانونية، (3)38، ص: 19 -57. تم الاسترجاع من الرابط التالي: https://doi.org/10.65088/2024.38.3.1

الاعتماد عند تحقُّق المخاطر، هذا عدا عن ارتباطه بإجراءات الرَّقابة البشريَّة ومُعالجة الشكاوى والإنصاف.[1]

ينتقل تقييم الأثر في اعتماد الرقابة من مرحلة ما بعد وقوع الضَّرر إلى مرحلة إدارة المخاطر قبل وقوعه. وتبقى قواعد القانون الإداري الأساسية وحماية البيانات والحقوق الأساسية وآليات القضاء الإداري جميعها عناصر مُكمّلة لنظام الرَّقابة، مع التأكيد أنَّ واقع الحال يُشير أنَّ القانون لا يعالج بصورةٍ كاملة مسائل الأساس القانوني للقرار الإداري الناتج عن الذكاء الاصطناعي، ولا التسبيب أو الوصول إلى الخوارزمية، وكذلك المسؤولية عن الضَّرر النَّاتج عنها.[2]

يترتَّب على ذلك عدم الاستغناء عن الإشراف البشري، حيث إنَّ هذا النظام لا يُمكن أن يحُل محلَّ السُلطة القانونية المُخوَّلة للموظَّف أو الجِهة الإدارية، ولا يمكن التخلِّي عن الرَّقابة البشريَّة، وبالتالي فإنَّ إعمال قواعد المسؤولية، ألزم القانون أن يكون هذا النظام مُصمَّماً بطريقةٍ يكون الأشخاص المُكلَّفون بالإشراف عليها لديهم إمكانية منع التَّدخُل فيه أو دخول النَّتائج السلبيَّة أو وقفه عند الحاجة، مع لُزوم تمتُّعِهم بالإشراف والتدريب والكفاءة، فضلاً عن تمتُّعِهم بالسُلطة الَّتي تُمكِّنهم من مُمارسة هذا الدور.

ثانياً: المسؤولية في ظل هذه الرقابة:

في الأصل إنَّ الرقابة ليست على مستوى موحَّد، أو تمَّ حصرها بقانونٍ واحد، إنَّما تجري حسب القانون الذي يُنظِّمها، واللائحة العامة لحماية البيانات GDPR وقواعد الحقوق الأساسية والمسؤولية عن المنتجات والقانون الإداري الوطني. أمَّا الضَّرر الذي يمكن وقوعه فقد يكون بسبب مخالفة قواعد السلامة والعيب الذي يُلازم القرار الإداري، واعتباره سبباً لطلب التعويض. يفرض القانون التزامات على الجهة التي تستخدم النظام، منها تقييم المخاطر والرَّقابة البشريَّة والمُراقبة بعد التشغيل، وأيضاً الاحتفاظ بسجلاتٍ مُعيَّنة، ووضع آلياتٍ للتَّعامل مع الحوادث والشكاوى؛ وعليه، فإنَّه لا يُمكن التذرُّع بأنَّ الخطأ كان خوارزمياً متى كان القانون يفرض عليها التزامات مُستقلَّة بشأن طريقة استخدام النَّظام ومُراقبته.

أشارت المادة (22) من اللائحة العامة لحماية البيانات GDPR على توفير حمايةٍ مُهمَّة ضدَّ القرارات القائمة حصراً على المعالجة الآلية، عندما يكون لها أثرٌ قانوني أو تأثيرٌ مُماثل جوهري على الشَّخص، مع وضع استثناءاتٍ مُحدَّدة وضمانات تتعلَّق بالتَّدخُل البشري، وإبداء الرأي والطَّعن في القرار. وقد جاء باتجاه ذلك قرار صادر عن محكمة العدل للاتحاد الأوروبي في قضيةٍ مُعيَّنة، حيث تعاملت مع نظام Scoring بوصفه من صور اتخاذ القرار الآلي، التي تدخل في نطاق المادة (22) من اللائحة، عندما تكون النتيجة الآلية ذات تأثير حاسم في القرار الذي يتَّخذه طرف آخر بشأن الشَّخص.[3]

وفي قرارٍ آخر صادر في 2025/2/27 يوضَّح أهميَّة الرَّقابة القضائية إذا تعلَّق النزاع بحق الشخص في الحُصول على معلومات ذات معنى عن المنطق المُستخدم في عمليَّة اتخاذ القرار الآلي، المُتعلِّقة بتقييم الجدارة الائتمانية. وقرَّرت المحكمة أنَّ المعلومات المُقدَّمة يجب أن تُشرح بطريقةٍ واضحة ومفهومة، الإجراءات والمبادئ الَّتي طُبِّقت فعلياً للوصول إلى النتيجة، وأنَّ مجرد صيغة رياضية مُعقَّدة أو الخوارزمية في صورتها التقنيَّة لا يكفي لتحقيق الشفافيَّة. وقرَّرت أنَّ الجِهة الرَّقابيَّة أو المحكمة، تستطيع أن توازن بين المصالح المُتعارضة لتحديد نطاق المعلومات المُتعارضة لتحديد نطاق المعلومات الواجب كشفها، وذلك عند وجود أسرارٍ تجارية أو حقوق للغير.[4]

يتبيَّن من ذلك أنَّ القرار الإداري القائم على خوارزمية، لا يمكن أن يتحوَّل إلى "قرارٍ غير قابل للفحص" بحجة السريَّة التَّقنيَّة. حيث إنَّه إذا كان الشخص المُتضرِّر لا يستطيع معرفة كيفية استخدام بياناته، أو كيفية الوصول إلى النتيجة الَّتي أضرَّت بمركزه القانوني، فإنَّ فعاليَّة الرَّقابة تصبح محدودة. وقد أيَّد الاتحاد الأوروبي هذا التَّفسير بمبدأ سيادة القانون، وفعاليَّة الرَّقابة

[1]- European Parliament and Council of the European Union, Regulation (EU) 2024/1689 of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), Official Journal of the European Union, OJ L, 2024/1689, 12 July 2024, Art. 3(1).

[2]- Mir, Oriol. (2025). "The AI Act from the Perspective of Administrative Law: Much Ado about Nothing?" European Journal of Risk Regulation, 16(1), 63–75. From the website below: https://doi.org/10.1017/err.2024.54.

[3]- Court of Justice of the European Union. (2023). Judgment of 7 December 2023, OQ v Land Hessen (SCHUFA Holding (Scoring)), Case C-634/21, ECLI: EU: C: 2023: 957. https://curia.europa.eu/.

[4]- Court of Justice of the European Union. (2024). Judgment of 18 January 2024, CROSS Zlín a.s. v Úřad pro ochranu hospodářské soutěže, Case C-303/22, ECLI: EU: C: 2024: 60. https://curia.europa.eu/.

القضائيَّة على الإدارة المؤتمتة.[1]

وفيما يتعلَّق بمسألة التَّعويض فقد أقرَّت المادة (82) من اللائحة GDPR أحقيَّة الشخص في التَّعويض عن الضَّرر المادي أو غير المادي الناشئ عن مُخالفة اللائحة. وقد أيَّد ذلك قرار محكمة العدل الصادر في 2023/5/4 أنَّ مُجرَّد مخالفة اللائحة لا يكفي وحده لنشوء حقَّه في التَّعويض، وإنَّما يجب تحديد الضَّرر والعلاقة السببيَّة بين المُخالفة والضَّرر؛ مع عدم جواز اشتراط بلوغ الضَّرر غير المادي درجةً مُعيَّنة من الجسامة كشرطٍ مُسبق للتَّعويض.[2]

تُقدّر المسؤولية كما أحكام المادة (82) من اللائحة متى توافرت شُروطها، وهذا يُشير أنها ذات طبيعة مُركَّبة ومُتعدَّدة المصادر، إذ تجمع بين الرَّقابة الإدارية الوقائية وبين الرَّقابة على البيانات وتلك القضائية، التي تقع على القرار الإداري والتَّعويض عن الضَّرر.

أمَّا بشأن إعمال قواعد هذه المسؤولية في الإمارات، فإنَّ المرسوم بقانون اتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية، يُمثِّل إحدى أهم مصادر الرَّقابة على استخدام الذكاء الاصطناعي، وذلك عندما يتم الاعتماد على إجراء تقييمٍ لأثر حماية البيانات، في حالات تشمل المُعالجة المنهجية والشَّاملة للجوانب الشخصيَّة باستخدام المُعالجة الآلية، وعندما يكون لها آثار قانونية أو أثر جسيم على صاحب البيانات. يشمل التَّقييم تحديد عمليات المُعالجة ومعرفة ضرورتها ومُلاءمتها، ومخاطرها المُتعلَّقة بالسريَّة والخُصوصيَّة، وتدابير مُعالجة الأضرار والمخاطر الصَّادرة ضدها.

أكَّدت المبادئ الحكومية الإماراتية أنَّ الإشراف البشري لا يزال ضرورياً لتصحيح الأخطاء والتَّحيُز، مع العِلم أنَّ الحوكمة والمُساءلة عنصران أساسيان في الاستخدام، ويمكن القول أنَّ معيار المسؤولية الإدارية الإماراتية تتَّجه إلى قواعد المسؤولية الإدارية المعطوفة على الالتزامات الخاصَّة بعملية البيانات والحوكمة الرقميَّة، وذلك بسبب عدم وجود تشريعٍ اتحادي خاص بالمسؤولية.

وتُراعى أحكام قانون المعاملات المدنية المرسوم بقانون اتحادي رقم (25) لسنة 2025، إذ يجب العودة إلى قانون المعاملات المدنية الجديد، والقواعد الخاصَّة بحسب طبيعة الضَّرر.

يبقى القرار الإداري الإماراتي مُتمتعاً بمشروعيته، إذ لا يجوز أن تجعل الإدارة من النَّظام والقرار الخوارزمي أن تصبح بديلاً عن الاختصاص القانوني، أو سبباً للإعفاء من التَّسبيب أو الرَّقابة. وقد أكَّدت دراسة حديثة ذات الصلة على ضرورة توافر الاختصاص والشكل والمحل والسبب والغاية، وأن تكون هناك حوكمة في الإجراءات ليكون القرار الصَّادر بمساعدة الذكاء الاصطناعي سليماً.[3]

أمَّا من الناحية القضائية فلم يظهر أي حكم اتحادي أو محلي حتى تاريخه، يؤسس نظاماً قضائياً مُستقلاً لمسؤولية الإدارة عن ضررٍ ناتج عن قرار إداري أصدره الذكاء الاصطناعي. لكنَّ القواعد والمبادئ موجودة، حيث إنَّه إذا ثبت أنَّ القرار الإداري استند إلى بياناتٍ خاطئة، أو نظامٍ غير صالح، أو نتيجة خوارزمية تمييزية أو لم يسمح بأي مراجعة بشريَّة رغم أهميته، فإنَّ ذلك يمكن أن يُشكِّل أساساً للطَّعن في القرار أو للمُطالبة بالتَّعويض حسب قواعد القانون.

وينبغي عند إصدار القرار الإداري مُراجعة اختصاص مصدر القرار، صحَّة الإجراءات، مشروعيَّة السبب، التَّحقُق من صحّة الوقائع الَّتي بُنِي عليها القرار، عدم انحراف السُلطة، التَّناسُب وحِماية الحقوق.

ونشير بأنَّ النظام الإماراتي يقوم على مزيجٍ من القواعد العامَّة للمسؤولية لناحية القرار الإداري وحماية البيانات بالنسبة لاستخدام الذكاء الاصطناعي، والأضرار النَّاتجة عنه. ويُشكِّل القانون 2021/45 أداةً مُهمَّة للرَّقابة الوقائية عندما تستخدم الإدارة المُعالجة الآلية، وتُمثِّل مصدراً مُهمَّاً للمبادئ المتعلَّقة بالشفافيَّة، والإشراف البشري والمُساءلة. وهذا الأمر يستدعي

[1]- Liga, Davide, (2024). The Interplay Between Lawfulness and Explainability in the Automated Decision – Making of EU Administration, in Governance of Automated Decision – Making and EU Law, Oxford University Press, pp: 239 – 264.

[2]- Court of Justice of the European Union. (2024). Judgment of 18 January 2024, CROSS Zlín a.s. v Úřad pro ochranu hospodářské soutěže, Case C-303/22, ECLI: EU: C: 2024: 60. From the website below: https://www.curia.europa.eu/

[3]- الواحدي، عبد الحميد أحمد. (2024) أركان القرار الإداري في عصر الذكاء الاصطناعي. المرجع السابق، ص 19.

العمل على تطوير نظامٍ مُتكامل للحوكمة والرَّقابة السَّابقة واللَّاحقة لا أن يكون تطبيق القواعد العامَّة بعد وقوع الضَّرر.

المبحث الثالث: المسؤولية الجنائية وإسناد الجريمة

تبقى جميع الجرائم الجناحية والجنائية المُتَّصلة باستخدام الخوارزميات ونظام الذكاء الاصطناعي خاضعة للتشريعات الجنائية الوطنية للدُّول الأعضاء. [1]

يعمد البعض على استخدام الذكاء الاصطناعي بهدف الإيذاء، وهذا الأمر أظهر السلوك الإجرامي، حيث تتعدَّد الاستخدامات والنتيجة واحدة، ألا وهي إحداث الضَّرر والإيذاء للبعض. حيث إنَّه من المُمكن أن ينتج محتوى تشهيري، تركيب صور مزيَّفة، ومقاطع فيديو مُنافية للأخلاق ضد شخصٍ حقيقي. أو أن يعمد إلى انتحال هوية شخص ما، أو ابتزاز أفراد للحُصول على أموالهم، أو كشف بياناتهم، أو خداعهم بعروضٍ وهميَّة واستغلالها بدون حق. أمَّا الصعوبة في هذا الأمر فتكمن في عدم إمكانية تحديد القرار الإجرامي، أو مدى إمكانية التَّمييز بين الاستخدام المشروع للتقنيَّة، أو تحديد الاستغلال الذي يُشكِّل جريمة.

والأصعب هو تحديد المسؤولية، حيث لا إنها لا تقوم إلَّا بمُجرَّد تحقُّق الضَّرر، إنما تتطلَّب ثُبوت وقوع الفِعل المادي المُجرَّم، وأيضاً المعنوي المُتمثِّل بالإرادة التي تدفع الفرد للقيام به، مع ضرورة احترام قرينة البراءة وقواعد إعمال المسؤوليَّة الجنائيَّة. وبالعودة إلى استخدام الذكاء الاصطناعي، فإنَّه لا يجوز اعتبار النِّظام ذاته فاعلاً جنائيَّاً مستقلاً، ولا يجوز افتراض مسؤولية المُطوِّر لمُجرَّد إنشائه النِّظام، أو تحميل المُستخدم مسؤولية لمُجرَّد أنَّه تصفَّح ذلك، لأنَّ التَّشريعات لا تعترف حتَّى اليوم بشخصيَّته الجنائيَّة. [2]

أولاً: أركان المسؤولية:

لكُل جريمة ركنين الأول مادي والثاني معنوي، وبالنسبة لهذا الأمر فإنَّ المسؤولية الجنائيَّة تقوم على إسناد الفِعل المُجرَّم إلى فردٍ لديه أهليَّة يضاف إلى الركنين المذكورين، حيث إنَّ مُخرجات الذكاء الاصطناعي الضَّارة لا تكفي وحدها لإسناد المسؤولية الجنائيَّة. إنَّما يجب تحديد إذا كان شخص طبيعي قد استخدم النِّظام بقصد ارتكاب الجريمة، أو ساهم بها أو ارتكب إهمالاً يُعاقب عليه القانون.

أمَّا لناحية المسؤولية فتكون حسب الحالة، إذا استخدم شخص النِّظام عمداً لارتكاب جريمة مثل تسجيل مقطع فيديو بغرض الابتزاز، فتكون المسألة في إثبات الجريمة المنسوبة إلى المُستخدم؛ أو أن يُنتج النِّظام مَخرجاً غير متوقَّع دون أن يُثبت أنَّ أي شخص قد ارتكب فعلاً تتوافر فيه عناصر الجريمة، في هذه الحالة لا يجوز تحويل مُجرَّد وقوع الضَّرر إلى افتراضٍ تلقائي لوجود جريمة.

وهناك حالة كأن يُسهم المُطوِّر أو المُشغِّل إلى تسهيل ارتكاب الجريمة من خلال فِعلٍ مُتعمَّد، أو خطأ يعاقب عليه القانون، في هذه الحالة يجب إثبات مُساهمة الشخص الآخر، وعلمه وخطئه حسب القانون الذي يُجرِّم الفعل.

تجدر الإشارة أنَّ المفاهيم التقليدية لهذه المسؤولية من فِعلٍ مادي وقصدٍ معنوي، وأيضاً السَّبب أو العلاقة السببيَّة، فإنَّه تواجه تحديَّات، لأنَّ النَّتيجة هي عملية حسابيَّة مُعقَّدة لا يمكن ردَّها بسهولة، أو اعتبارها نتاج بشري مُنفرد.

يتمثَّل الركن المادي من خلال ارتكاب فعلٍ كإنشاء محتوى غير مشروع، استخدام بيانات الغير، التَّشهير، الاحتيال. وفي هذه الحالة لا يُشترط أن يكون الفاعل قد أنشأ هذه المُخرجات بنفسه من النَّاحية التقنيَّة، حيث إنَّ ذلك يتطلَّب إنشاء نظام توليدي، يتمثَّل في طلب إنشاء المحتوى ثم نشره أو استخدامه ضدَّ شخصٍ آخر، وهذا يتطلَّب أفعال مُتعدَّدة وليس فِعلٍ واحد فقط.

أمَّا الركن المعنوي فيكون بالتَّصوُر العمدي ووجوب إثبات القصد، أي أن يكون بِعلم وإرادة الفاعل الذي تتّجه نتيجته إلى

[1]- European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689, 12 July 2024. https://eur-lex.europa.eu/eli/reg/2024/1689/oj.

[2]- Giannini, Alice. (2021). "Artificial Intelligence, Human Oversight, and Criminal Liability: A European 'Strength Test'?" Criminalia, 249–274. From the website below: https://cris.maastrichtuniversity.nl/en/publications/intelligenza-artificiale-human-oversight-e responsabilit%C3%A0-penale.

الضَّرر. حيث إنَّه ينبغي التَّحقُق من ثُبوت الوقائع والقرائن وتوافر عناصر المُساهمة الجنائيَّة المطلوبة، عندما يكون مُطوّر النِّظام قد توقَّع إمكانية إساءة استخدام النِّظام بصورةٍ عامَّة، لإثبات اشتراكه في جريمةٍ مُحدَّدة، أو أنَّ الخطأ التَّقني والعِلم به أدى إلى ارتكاب فعلٍ مُعيَّن آخر بشخصٍ آخر. [1]

تقع المسؤولية على المُستخدم إذا ثبت أنَّه ارتكب بنفسه السُلوك المُجرَّم أو ساهم فيه وفق أحكام القانون. أمَّا مسؤولية المُطوَّر فتكون عند إثبات سُلوكٍ يدخل في نظام التَّجريم، كالمُساهمة العمديَّة في فِعلٍ غير مشروع. ومن ناحية مسؤولية المُشغّل فإنَّه يتوقَّف على دوره الفعلي، وعلمه بالواجبات القانونية المفروضة عليه، وهذا يُشير إلى أنَّ مسؤولية كُل فرد منهم تحتاج إلى أساسٍ قانوني مُستقل.

نصَّ المرسوم بقانون اتحادي رقم (34) لسنة 2021 بشأن مكافحة الشائعات والجرائم الإلكترونية على حكم يتعلَّق بالشَّخص المسؤول عن الإدارة الفعليَّة للشخص الاعتباري في نطاق الجرائم الَّتي يُنظِّمها القانون، ويُطبَّق ذلك حسب الشُروط دون اعتباره قاعدة تُتيح المُساءلة ضدَّ أي شخص بِحُكم مسؤوليَّته الوظيفيَّة.

ثانياً: المسؤولية عن الجرائم:

أ. التشهير:

إذا ما حدث تشهير باستخدام الذكاء الاصطناعي عبر استخدام تسجيلٍ صوتي أو مرئي أو نسب واقعة لشخصٍ ما أساءت له ولاعتباره، ومن ثم جرى إعادة نشر على نحوٍ يُحقِّق العناصر المُقرَّرة في القانون الجنائي؛ فإنَّه ينبغي التَّحقُق من نص القانون المحلِّي وطبيعة الإسناد ووسيلة النشر والقصد والدَّوافع وراء الفِعل.

اعتبرت المادة (34) جريمة السَّب والقذف المُركَّبة باستخدام شبكةٍ معلوماتية، أو وسيلة تقنية معلومات أو نظام معلوماتي. يكون النَّص ذات صلة إذا استخدم نظام الذكاء الاصطناعي لإنتاج أو محتوى تشهيري أو التَّلاعُب به، ومن نشره أو إرساله على نحوٍ تتحقَّق فيه عناصر الجريمة. وفي هذه الحالة يتم البحث فيمن ساهم في المُحتوى أو من ساهم في نشره، أو إحداث الفِعل المُجرَّم ومن ظُروف الواقعة.

ونصَّت المادة (52) بأنَّه لا ينبغي دمج كل مُحتوى غير صحيح في جريمةٍ واحدة، إذ يجب التَّمييز بين كُل فِعل حيث لكلٍ منهم ظُروفه وعناصره وشُروطه. (مثل: الاعتداء على السُمعة، التَّشهير، نشر الأخبار المُضلِّلة، الاحتيال) كما المرسوم بقانون اتحادي رقم (34) لسنة 2021 بشأن مكافحة الشائعات والجرائم الإلكترونية.

أمَّا من ناحية قانون الاتحاد الأوروبي فإنَّه لا يوجد نص موحَّد يجمع كُل صور الجرائم والأضرار عن استخدام الذكاء الاصطناعي، حيث إنَّه يتوقَّف التَّجريم والعقوبة على القانون الجنائي الوطني والقواعد المُتعلِّقة بحماية البيانات والحقوق الأساسية. ولا يُعد قانون الذكاء الاصطناعي الأوروبي قانوناً عاماً لهذه الناحية، فبحسب المادة (50) منه، فإنَّها تُقرَّر التزامات شفافيَّة تتعلَّق بالمُحتوى، ومنها الإفصاح عن بعض صُور التَّزييف العميق (deep fakes) من غير الخلط بين الإخلال بالتزام الإفصاح وبين جريمة التَّشهير، حيث لكلٍ منهما أساسه القانوني. [2]

ب. انتهاك الخصوصية:

نصَّت المادة (44) من المرسوم بقانون اتحادي رقم (34) لسنة 2021 الإماراتي على أنه تكون ذات صلة بنشر صور أو معلومات خاصَّة جرى توليدها أو تعديلها اصطناعياً، متى تحقَّقت عناصر النَّص وظُروفه. وقد تناولت هذه المادة الاعتداء على الخصوصيَّة، أو حُرمة الحياة الخاصَّة باستخدام شبكةٍ معلوماتية، أو نظامٍ معلوماتي أو وسيلة تقنيَّة المعلومات. هذا بالإضافة إلى موادٍ أخرى منها الاعتداء على البيانات والمعلومات الشخصيَّة، (المواد 6، 12، 13، 45 من المرسوم بقانون اتحادي رقم (34) لسنة 2021).

[1]- European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Ibid.

[2]- European Parliament and Council of the European Union, Regulation (EU) 2024/1689 of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act), Official Journal of the European Union, OJ L, 2024/1689, 12 July 2024, Art. 3(1).

أمَّا بحسب القانون الأوروبي واللائحة، فإنَّ هذه الأخيرة لا تُجرِّم كُل معالجة غير مشروعة بذاتها، باعتبارها جريمة، وقد أجازت المادة (84) بأنَّه للدُّول الأعضاء وضع قواعد بشأن العقوبات الأخرى المُنطبقة على انتهاكات اللائحة، إذ إنَّ ذلك يؤدي إلى تدابير إدارية أو تعويضٍ مدني؛ في المقابل فإنَّ الفِعل يحتاج إلى وجود نصٍ جنائي واجب التطبيق.

وبحسب الاتحاد الأوروبي وبشكلٍ عام فإنَّ المسؤولية تكون بحسب البيانات وطبيعة الجهة الَّتي تُعالجها، وكذلك اللائحة العامَّة، حيث تخضع لمعالجة البيانات من قِبل السُلطات المُختصَّة لأغراض منع الجرائم والتّحقيق فيها ومُلاحقتها.

أمَّا القانون الإماراتي فقد تضمَّن نصوصاً مُستقلة، وتكمن الأهمية لهذه النصوص كونها ترتكز على الفِعل المُرتكب باستخدام التقنيَّة، ولا يلزم أن يكون قد ابتكر نظام الذكاء الاصطناعي بنفسه حتى يخضع للمُساءلة إذا ثبت ارتكابه فِعلاً مُجرَّماً من خلاله.

وبشكلٍ عام، فإنَّه لا يصح وصف الأحكام الأوروبية بأنَّها أحكام جنائيَّة مُباشرة عن جرائم ارتكبت بواسطة الذكاء الاصطناعي، فقد صدر قرار عن محكمة العدل الأوروبية بتاريخ 2023/1/26 تناول معالجة البيانات البيومترية في سياق إجراءاتٍ جنائيَّة، وفسَّر شرط مشروعيَّة هذه المعالجة في ضوء التوجيه 2016/680 وميثاق الحقوق الأساسية للاتحاد الأوروبي. أمَّا أهميَّته فتتمثَّل في تأكيد مسألة جمع البيانات ومُعالجتها، وبأنَّه لا ينبغي أن ينفصل الأساس القانوني والضمانات المطلوبة، وأنَّ استخدام هذه الوسائل لا يرفع القيود المفروضة على السُلطات. [1]

ينبغي التطرُّق لموضوع الإثبات، حيث إنَّه يعد إحدى التحديَّات العمليَّة، حيث إنَّ المخرج الذي أنشئ نموذج خارجي أو مُعدَّل عنه، أو أي فعل ذات صلة له وصف جُرمي، وهذا الأمر لا يكفي بأنَّ يتم الاعتماد على المحتوى الظَّاهر بحدِ ذاته، إنَّما ينبغي أن يتم فحص القرائن الرقميَّة الَّتي تُساعد في تحديد المنشأ والمُستخدم وسياق الإنتاج.

أمَّا الأدلَّة ذات الصلة، فإنها تتَّصِل بظروف الواقعة، سجلات البيانات، توقيت الإنشاء والنشر، سجل المحادثة مع النظام، بيانات الملفات الوصفيَّة، عمليات الدَّفع والتَّحويل وغيرها من الأمور، هذا فضلاً عن توافر أي دليل يُثبت الغرض من إنشاء المحتوى أو استخدامه. إذ يجب جمع الأدلَّة وحِفظها مع مُراعاة الخصوصيَّة وسريَّة البيانات وحقوق الدفاع.

يُفيد الكشف التَّقني أنَّ الصوت والصورة مولَّدان بالذكاء الاصطناعي، وقد يثبت طبيعة المحتوى لكنَّه لا يُحدَّد من أنشأه أو نشره أو كان عالماً بكذبه، حيث يجب أن توجد احتمالات جديَّة للاختراق أو الاستعمال من الغير، إذا كان ذلك بواسطة حسابٍ إلكتروني خاص. الأمر الذي يتطلَّب اعتماد تقييمٍ مُتكامل للأدلَّة التقنيَّة والبشريَّة وعدم تحويل احتمالات التَّحليل الخوارزمي إلى قرينةٍ قاطعة على الفِعل المُجرَّم.

خاتمة

تناولت هذه الدراسة موضوع "المساءلة القانونية عن أضرار الذكاء الاصطناعي والخوارزميات: دراسة مقارنة في المسؤولية الجزائية والمدنية والإدارية بين الاتحاد الأوروبي والإمارات العربية المتحدة" وقد خلصت أنَّ المسؤولية القانونية عن الأضرار لا تتحدَّد بمُجرَّد اعتبار الضَّرر صدر عن مُخرجاتٍ خوارزمية، إذ يتطلَّب الأمر النَّظر أيضاً في طبيعة البيانات وسلامتها والحقوق والمصالح التي وقع عليها الضَّرر، مع ضرورة تحديد الطَّرف الذي أسهم في حُدوثه، ومدى إمكانية إسناد الفِعل قانوناً. مع الإشارة إلى أن البيانات الشخصية وجميع المعلومات المُتعلِّقة بالحياة الشخصيَّة والسُمعة والهويَّة وغيرها من الاعتبارات المِهنيَّة والمالية، التي قد تتعرَّض للانتهاك أو الاستغلال أو الاحتيال، فمن ناحية يتوجَّب الإفصاح عن البيانات ومن ناحيةٍ أخرى قد يتم استخدام بعض المعلومات لأهدافٍ غير سامية ومُعاقب عليها قانوناً.

أمَّا المسؤولية فتكون نتيجة تفاعُلٍ بين البيانات المُخلَّة والتَّصميم الخوارزمي، وأيضاً التَّدريب والتَّحديث وطريقة التَّشغيل، حيث يتوجَّب تحديدها إذا ما أدَّت إلى ضررٍ مادي أو معنوي يمُس بالخصوصيَّة والكرامة والاعتبار؛ ويجب البحث في مشروعية الفِعل أو السُلوك ومدى توقُّع الضَّرر، ومدى إمكانية تفاديه والعلاقة السببيَّة بين الفِعل والنتيجة.

[1]- Court of Justice of the European Union. (2023). Judgment of 26 January 2023, Criminal proceedings against V.S. (Ministerstvo na vatreshnite raboti), Case C-205/21, ECLI: EU: C: 2023: 49, from the website below: https://www.eur-lexeuropa.eu/.

وحيث إنَّ لِكُل ضرر مسؤولية مُعيَّنة، تقوم المسؤولية المدنية وتُعد أساساً مُهماً للمُطالبة بالتَّعويض عن الضَّرر المادي أو المعنوي، كما تناولها قانون الذكاء الاصطناعي الأوروبي واللائحة العامة GDPR، وبحسب القانون الإماراتي فيعمل بأحكام المرسوم بالقانون الاتحادي رقم (45) لسنة 2021 بشأن حماية البيانات الشخصية، وهذا ما يُكرِّس أعمال المسؤولية المدنية.

وبالمقارنة بين قواعد المسؤولية المُتعلِّقة بالتَّشريعين، فإنَّه يقتضي الأمر التَّمييز بين المسؤولية عن مُعالجة البيانات ذاتها، والمسؤولية عن مُحتوى المُخرجات الخوارزمية، فالضرر قد ينشأ من انتهاك قواعد حماية البيانات، أو بسبب مُحتوى يمُس السُمعة أو الخصوصيَّة أو انتحال الهويَّة، وينبغي العِلم بأنَّ كُل صورة لها تكييفها وشروطها القانونيَّة الخاصَّة.

ومن ناحية المسؤولية الإدارية، فتكون من واجبات الامتثال والشفافيَّة والأمن وإدارة المخاطر والرقابة على الأنظمة، وجميعها واجبات نظمها قانون الاتحاد الأوروبي واللائحة العامَّة في المادة (99) منه.

أمَّا القانون الإماراتي رقم (34) لسنة 2021 فإنَّه يتضمَّن أحكاماً تتصِّل بالاحتيال الإلكتروني، والاعتداء على الخصوصيَّة والسَّب والقذف، وصور التعامل غير المشروع مع البيانات والمعلومات، وهذا الأمر يقتضي التَّحقُّق من انطباق النص على السُلوك المُحدَّد وإثبات أركان الجريمة، والقصد الجنائي مع تحديد دور المُستخدم أو المُطوَّر أو المُزوّد، وذلك دون افتراض المسؤولية الجنائية لِمُجرَّد وجود صلةٍ تقنيَّة بالنظام.

تجدر الإشارة أنَّ القانون الأوروبي لا ينشئ نظام موحَّد شامل للجرائم والعقوبات الجنائية عن جميع الأفراد، حيث إنَّه ركَّز على تنظيم الأنظمة والالتزامات الرقابيَّة والجزاءات، أمَّا التَّجريم والعقاب فهما خاضعين للتشريعات الجنائيَّة الوطنية. تتطلَّب الحماية الفعَّالة للمُتضرَّر منظومة متكاملة من تطوير القواعد الإجرائية المتعلِّقة بإثبات الضَّرر والسببيَّة في البيئات الخوارزمية، وتوضيح واجبات الأطراف مُقدّمِي الأنظمة ومُشغِليها ومُستخدميها، وتحسين التَّنسيق بين سُلطات حماية البيانات والجهات الرَّقابية والسُلطات القضائيَّة مع ضمان حق المُتضرَّر في الانتصاف الفعَّال، وعدم تحميله وحده عبء إثبات المسائل التقنيَّة التي لا يستطيع الوصول إلى أدلَّتها. وبذلك لا ينبغي تعقيد أو تعدُّد المُتدخلين فيها إلى إهدار الحقوق أو خلق فراغٍ في المُساءلة، إنَّما يجب أن يظلَّ استخدامها خاضعاً لمبادئ المشروعية والتناسُب والشفافيَّة، وحماية الحقوق الأساسية في ضَوء التَّشريعات الأوروبية والإماراتية كُلٌ بحسب نطاقه وشُروط تطبيقه.

أبرز التوصيات

- تطوير التَّشريعات القانونية في كُلٍ من الاتحاد الأوروبي والإمارات العربية المتحدة بما يضمن تنظيم المسؤولية عن الأضرار النَّاشئة عن الذكاء الاصطناعي، ومدى مساهمته في وقوع الضرر وتوقعه أو منعه.
- تحديد المسؤولية للأطراف المعنيَّة ومساهمة كُل طرف فيها بشكلٍ مُفصّل ومُوسَّع.
- تعزيز الضمانات المُتعلِّقة بحماية البيانات الشخصيَّة والخصوصيَّة، ومدى حماية السريّة عبر فرض التزاماتٍ واضحة مُتعلِّقة بمشروعيتها ومُعالجتها وتخزينها، والحدّ من استخدامها ضدَّ الأفراد وحقوقهم.
- تحقيق الرَّقابة الإدارية عبر دعم استقلال الجهات الرقابيَّة، والتَّدقيق على مُخرجات أنظمة الذكاء الاصطناعي، وفرض الجزاءات الإدارية بشكلٍ استنسابي مع طبيعة المُخالفة وخُطورتها، كما هو موضَّح في التَّشريعات ذات الصلة.
- تطوير الإطار القانوني للمُساءلة الجنائيَّة عبر توضيح شروط إسناد الجرائم المُرتكبة من خلال استخدام أنظمة الذكاء الاصطناعي إلى الأشخاص الطبيعيين أو الاعتباريين، وضمان عدم افتراض المسؤولية الجنائيَّة، لمُجرَّد المُشاركة في تطوير النظام متى توافرت أركان الجريمة وقواعد المسؤولية عنها.
- دعم التعاون القضائي والبحثي بين الاتحاد الأوروبي وكذلك الإماراتي عبر تعزيز وتطوير آليات حِفظ الأدلَّة الرَّقميَّة، وإثبات مصدر المُخرجات الخوارزمية لدعم فعاليَّة التَّحقيق والمُلاحقة، وفرض عقوبات بحق الفاعلين، والعمل على صون حقوق المُتضرّرين.

المراجع

المراجع باللغة العربية:

- الشامسي، ريم غريب، (2022). حماية الخصوصية الرقمية في ظل تطبيقات الذكاء الاصطناعي: دراسة تحليلية مقارنة، رسالة ماجستير في القانون الخاص، كلية القانون، جامعة الإمارات العربية المتحدة، الإمارات العربية المتحدة.
- الظهوري، فهد سعيد، والنجيفي، مصطفى سالم مصطفى. (2024). مسؤولية الإدارة عن استخدامات الذكاء الاصطناعي على أساس الخطأ. مجلة جامعة الشارقة للعلوم القانونية، 21(1)، https://doi.org/10.36394/jls.v21.i1.12
- مجمع اللغة العربية بالقاهرة، (2012). معجم مصطلحات الحاسبات بالمجمع، القاهرة، ط4.
- النقبي، محمد سالم، وعثمان، أيمن. (2024). المسؤولية المدنية الناشئة عن أضرار تطبيقات الذكاء الاصطناعي في مهنة أعمال المحاماة: دراسة مقارنة بين القانون الإماراتي والأوروبي، مجلة جامعة الشارقة للعلوم القانونية، مجلد 21، العدد 4.
- الواحدي، عبد الحميد أحمد. (2024). أركان القرار الإداري في عصر الذكاء الاصطناعي. مجلة جامعة الإمارات للبحوث القانونية، 38(3)، تم الاسترجاع من الرابط التالي: https://doi.org/10.65088/2024.38.3.1

المراجع باللغة الأجنبية:

- Aboelazm, Karem Sayed, Khalid Mohamed Dganni, Sumaya Aljahoori, and Zahid Hussain, "ChatGPT and the Erosion of Confidentiality: Legal and Ethical Implications of Generative AI Use in Public Office," International Journal of Law and Management, 2026, pp. 1–26, from the website below: https://doi.org/10.1108/IJLMA-02-2026-0097
- Abouhaiba, Nagwa, Saed Ahmed Khouli, and Maya Khater, "Towards Protecting the Injured Party from Errors and Hallucinations of Artificial Intelligence: A Contemporary Legal Perspective," F1000Research, Vol. 15, 2026, Article 569, from the website below: https://doi.org/10.12688/f1000research.179603.1
- Almaazmi, Nada Mohamed, "Processing Personal Data Without the Data Subject's Consent in Light of Federal Decree-Law No. 45 of 2021," UAEU Law Journal, Vol. 40, No. 1, 2026, from the website below: https://doi.org/10.65088/2026.40.1.3
- Arnold, David, Will Dobbie, and Peter Hull, "Measuring Racial Discrimination in Algorithms," AEA Papers and Proceedings, Vol. 111, May 2021, from the website below: https://doi.org/10.1257/pandp.20211080
- Bertolini, Andrea, Artificial Intelligence and Civil Liability, European Parliament, Policy Department for Citizens' Rights and Constitutional Affairs, Brussels, 2020, from the website below: DOI: https://doi.org/10.2861/220466
- Bygrave, Lee A., "Article 22: Automated Individual Decision-Making, Including Profiling," in Christopher Kuner, Lee A. Bygrave, and Christopher Docksey (eds.), The EU General Data Protection Regulation (GDPR): A Commentary, Oxford University Press, Oxford, 2020.
- Chemlali, Laroussi, "La prise de décision automatisée: Une analyse comparative entre le RGPD européen et le Décret-loi fédéral émirati n° 45 de 2021," University of Sharjah Journal of Legal Sciences, Vol. 23, No. 1, 2026, from the website below: https://doi.org/10.36394/jls.v23.i1.28

- Chesterman, Simon, "Lawful but Awful: Evolving Legislative Responses to Address Online Misinformation, Disinformation, and Mal-Information in the Age of Generative AI," The American Journal of Comparative Law, Vol. 72, No. 4, 2024, from the website below: https://doi.org/10.1093/ajcl/avaf020
- Court of Justice of the European Union. (2023). Judgment of 26 January 2023, Criminal proceedings against V.S. (Ministerstvo na vatreshnite raboti), Case C 205/21, ECLI:EU:C:2023:49, From the website below: https://www.eur-lexeuropa.eu /
- Court of Justice of the European Union. (2023). Judgment of 7 December 2023, OQ v Land Hessen (SCHUFA Holding (Scoring)), Case C 634/21, ECLI: EU: C: 2023: 957. https://curia.europa.eu/
- Court of Justice of the European Union. (2024). Judgment of 18 January 2024, CROSS Zlín a.s. v Úřad pro ochranu hospodářské soutěže, Case C 303/22, ECLI: EU: C: 2024: 60. From the website below: https://www.curia.europa.eu/
- Elham Tabassi, Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1, National Institute of Standards and Technology, Gaithersburg, Maryland, 2023.
- Ernst Karner, Bernhard A. Koch, and Mark A. Geistfeld, Comparative Law Study on Civil Liability for Artificial Intelligence, European Commission, Directorate-General for Justice and Consumers, 2021.
- European Parliament and Council of the European Union. (2024). Regulation (EU) 2024/1689 of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union, L 2024/1689, 12 July 2024. https://eur-lex.europa.eu/eli/reg/2024/1689/oj
- Fernández Llorca, David, Vicky Charisi, Ronan Hamon, Ignacio Sánchez, and Emilia Gómez, "Liability Regimes in the Age of AI: A Use-Case Driven Analysis of the Burden of Proof," Journal of Artificial Intelligence Research, Vol. 76, 2023, from the website below: https://doi.org/10.1613/jair.1.14565
- Fossati, Curzio, "AI Systems and Product Liability in the EU: A Private International Law Analysis," EU and Comparative Law Issues and Challenges Series (ECLIC), Vol. 9, 2025, from the website below: https://doi.org/10.25234/eclic/38130
- Garfield Tenzer, Leslie Y., "Defamation in the Age of Artificial Intelligence," New York University Annual Survey of American Law, Vol. 80, No. 2, 2024.
- Giannini, Alice. (2021). "Artificial Intelligence, Human Oversight, and Criminal Liability: A European 'Strength Test'?" Criminalia. From the website below: https://cris.maastrichtuniversity.nl/en/publications/intelligenza-artificiale-human-oversight-e-responsabilit%C3%A0-penale
- Holtz, Hajo Michael, and Jonas Ledendal, "AI Data Governance – Overlaps Between the AI Act and the GDPR," Law, Innovation and Technology, Vol. 18, No. 1, 2026, from the website below: https://doi.org/10.1080/17579961.2026.2633677

- Lee, Kyung-Min, "A Study on the Use of Generative AI and Protection of Trade Secrets," Legal Theory & Practice Review, Vol. 12, No. 4, 2024, from the website below: https://doi.org/10.30833/LTPR.2024.11.12.4.205.
- Lidsky, Lyrissa Barnett, and Andrew Daves, "Inevitable Errors: Defamation by Hallucination in AI Reasoning Models," Journal of Free Speech Law, Vol. 6, 2025.
- Liga, Davide, (2024). The Interplay Between Lawfulness and Explainability in the Automated Decision – Making of EU Administration, in Governance of Automated Decision – Making and EU Law, Oxford University Press, pp: 239 – 264.
- Mayrhofer, Ann-Kristin, "AI Act and New Product Liability Directive: The Interplay Between AI Safety Regulation and Compensation," Cambridge Forum on AI: Law and Governance, Vol. 2, 2026, Article e13, from the website below: https://doi.org/10.1017/cfl.2026.10048
- Mir, Oriol. (2024). "Algorithms, Automation, and Administrative Procedure at EU Level." In Herwig C. H. Hofmann and Felix Pflücke (eds.), Governance of Automated Decision-Making and EU Law (pp. 52–77). Oxford University Press. From the website below: https://doi.org/10.1093/9780198919575.003.0003
- Mir, Oriol. (2025). "The AI Act from the Perspective of Administrative Law: Much Ado about Nothing?" European Journal of Risk Regulation, 16(1). From the website below: https://doi.org/10.1017/err.2024.54
- National Institute of Standards and Technology (NIST), AI Risk Management Framework (AI RMF) Resources: Executive Summary, Artificial Intelligence Resource Center (AIRC), 2023. From the website below: https://circ.gov/
- Novelli, Claudio, Federico Casolari, Philipp Hacker, Giorgio Spedicato, and Luciano Floridi, "Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity," Computer Law & Security Review, Vol. 55, November 2024, Article 106066, https://doi.org/10.1016/j.clsr.2024.106066
- Organisation for Economic Co-operation and Development (OECD), Explanatory Memorandum on the Updated OECD Definition of an AI System, OECD Publishing, March 2024, No. 8. Accessed on: 1/9/2026. From the below website: https://www.oecd.org/
- Redka -Ligarska, Iwona, "Employer as an AI System Operator and Tortious Liability for Damage Caused by AI Systems: European and US Perspectives," The Chinese Journal of Comparative Law, Vol. 12, Oxford University Press, 2024, from the website below: https://doi.org/10.1093/cjcl/cxae015
- Salmond, John W., Jurisprudence, 4th ed., Stevens and Haynes, London, 1913, available on Scribd. Accessed on: 1/9/2026. From the website below: https://www.scribed.com/
- Stanford Encyclopedia of Philosophy, "The Philosophy of Computer Science," 2013. Accessed on: 1/9/2026. From the website below: https://www.plato.stanford.edu/

- Sun, Haochen, "Regulating Algorithmic Disinformation," Columbia Journal of Law & the Arts, Vol. 46, No. 4, 2023, from the website below: https://doi.org/10.52214/jla.v46i3.11237
- Union Properties PJSC & Anor v Trinkler & Partners Ltd & Others, ADGMCFI 0010 (Court of First Instance, Abu Dhabi Global Market, 6 March 2026.
- United Arab Emirates, Federal Decree-Law No. (45) Of 2021 Concerning the Protection of Personal Data, Articles 1–5, Official Legislation Portal of the United Arab Emirates, 2021.
- Xenidis, Raphaële, "Tuning EU Equality Law to Algorithmic Discrimination: Three Pathways to Resilience," Maastricht Journal of European and Comparative Law, Vol. 27, No. 6, 2020, from the website below: https://doi.org/10.1177/1023263X20982173
- Zech, Herbert, "Liability for AI: Public Policy Considerations," ERA Forum, Vol. 22, No. 1, 2021, from the website below: https://doi.org/10.1007/s12027-020-00648-0