التنظيم القانوني للتزييف العميق في قانون الذكاء الاصطناعي الصادر عن الاتحاد الأوروبي

The Legal Regulation of Deepfake in the European Union Artificial Intelligence Act

د. محمود حسين سيد أبوسيف

المدرس بقسم القانون الدولي العام

كلية الحقوق – جامعة بني سويف

ملخص البحث:

يُعتبر التزييف العميق واحداً من أكثر أنظمة الذكاء الاصطناعي انتشاراً في العصر الحالي. فمع سهولة استخدامه، وانخفاض تكلفته، وإتاحته للجميع، أصبح من أسهل الطرق المستخدمة لخداع المتلقين. وعلى الرغم من وجود جوانب إيجابية لاستخدام هذه التقنية في العديد من المجالات، وخاصة في المجالات العلمية والترفيهية، إلا أنه قد يُستخدم لتحقيق أضرار عديدة. فقد يؤدي استخدام هذه التقنية إلى تحقيق أضرار اقتصادية وسياسية واجتماعية وأمنية على المستويين الداخلي والدولي.

وقد تنبه الاتحاد الأوروبي إلى خطورة أنظمة الذكاء الاصطناعي بشكل عام، والتزييف العميق بشكل خاص، وتبنى، نتيجة لذلك، اللائحة رقم ١٦٨٩/٢٠٢٤، أو ما يُسمى بـ "قانون الذكاء الاصطناعي"، والذي يُعتبر أول إطار قانوني واسع النطاق لتنظيم مجموعة متنوعة من أنظمة الذكاء الاصطناعي في جميع أنحاء الاتحاد الأوروبي. ويتبنى هذا القانون نهجاً قائماً على المخاطر، حيث صُنفت أنظمة الذكاء الاصطناعي إلى فئات محددة تختلف القواعد القانونية المطبقة عليها، وذلك بتقسيمها إلى ممارسات محظورة، وأنظمة عالية الخطورة، وأنظمة أخرى تتطلب التزامات معينة.

ويهدف هذا البحث إلى دراسة التنظيم القانوني لتقنية التزييف العميق في هذا القانون، وذلك من خلال تناول ماهية هذه التقنية وأهم خصائصها التي تميزها عن غيرها من تقنيات الذكاء الاصطناعي في القسم الأول. ثم نتناول في القسم الثاني القواعد القانونية المطبقة على هذه التقنية، والتزامات المستخدمين ومقدمي الخدمة، والعقوبات المطبقة في حالة مخالفة هذه الالتزامات.

الكلمات المفتاحية: التزييف العميق – الذكاء الاصطناعي – الاتحاد الأوروبي.

Abstract:

Deepfake is one of the most prevalent Artificial Intelligence (AI) systems today. Due to its usability, low cost, and accessibility, it has become one of the easiest ways to deceive recipients. Although there are positive impacts of this technique in many fields, especially in scientific and entertainment sectors, it can also lead to harmful consequences. Therefore, the use of this technique can result in economic, political, social, and security damages at both national and international levels.

The European Union (EU) has recognized the seriousness of AI systems in general, and deepfake technology in particular. As a result, it adopted Regulation (EU) 2024/1689, known as the EU AI Act, which is considered the first comprehensive legal framework for the regulation of AI systems across the EU. This Act adopts a risk-based approach that classifies AI systems into specific categories, each with different applicable legal rules. The classifications include prohibited practices, high-risk AI systems, and obligations for certain AI systems.

This research aims to study the legal regulation of deepfake under the EU AI Act. In the first part, it will explain the definition of this technique and its main characteristics. The second part will discuss the applicable legal rules governing this technique, the obligations of providers and deployers, and the penalties for violations of these obligations.

Keywords: Deepfake – Artificial Intelligence – The European Union.

مقدمة

لقد تَقَدَّمَتِ التكنولوجيا بطرقٍ أصبحت تطمس الخطوط الفاصلة بين ما هو حقيقي وما هو مُحاكَى، وأصبحت تقنيات الذكاء الاصطناعي تتطور بشكل سريع لتحقيق فوائد ومميزات للمستخدمين إلا أن ذلك لم يمنع من ظهور جانب سلبي لهذه التقنيات، بحيث يتم استخدامها لإحداث أضرار جسيمة. ومن أهم هذه التقنيات ما يسمى بالتزييف العميق (Deepfake)، وهي عبارة عن تقنية تتضمن إنشاء مقاطع فيديو، أو صور، أو مقاطع صوتية، أو التلاعب بمحتوى أصلى موجود بالفعل، بحيث يصعب على الشخص العادي التعرف على أن هذا المحتوى مزيف أو غير حقيقي. وقد يؤدي هذا إلى عواقب لا حصر لها، والتي قد تشمل استخدام أدلة مزورة في المحاكم، أو ممارسات انتخابية غير عادلة، أو إثارة الرعب والفزع بين الأفراد.

وبذلك تُعتبَر تقنية التزييف العميق واحدة من أكبر التهديدات للمجتمع في الوقت الحالي نظراً لما تقوم به هذه التقنية من طمس للخط الفاصل بين الحقيقة والخيال، مما يزيد من المخاوف بشأن انتهاك الخصوصية والتعدي على الحقوق الأساسية وزيادة التهديدات الأمنية ويؤثر على ثقة الجمهور في وسائل الإعلام أو الشخصيات العامة، بل والإضرار بأمن الدول في بعض الحالات.

وأمام الفراغ التشريعي لتنظيم استخدام هذه التقنية، استخدمت التشريعات الحالية، مثل القوانين الجنائية وتشريعات حماية البيانات، للتخفيف من المخاطر المرتبطة بها والحد منها. ومع ذلك، فإن هذه القوانين لم تكن كافية لمعالجة التحديات المتعددة التي تفرضها هذه التقنية، مما سلّط الضوء على الحاجة المُلِحة إلى تشريعات أقوى لحماية المستخدمين من مخاطر هذه التقنية وما قد

ينتج عنها من أضرارٍ وخيمة. لذلك، كان من الضروري وضع قواعد قانونية خاصة لتنظيم تقنية التزييف العميق مع استمرارها في الانتشار والتطور السريع.

وقد تنبّه الاتحاد الأوروبي لأهمية هذه التقنية كأحد المخاطر التي تفرضها أنظمة الذكاء الاصطناعي على دول الاتحاد الأوروبي، نظراً لما قد يكون لها من عواقب ضارة ومسيئة يجب تنظيم استخدامها أو حظرها في بعض الحالات لأنها تتعارض مع قيم الاتحاد المتمثلة في احترام كرامة الإنسان والحرية والمساواة والديمقراطية وسيادة القانون والحقوق الأساسية المنصوص عليها في ميثاق الحقوق الأساسية للاتحاد الأوروبي، بما في ذلك الحق في عدم التمييز وحماية البيانات والخصوصية وحقوق الطفل[١].

ونتيجة لذلك، اعتمد الاتحاد الأوروبي اللائحة رقم ١٦٨٩/٢٠٢٤، والتي سُميت بـ 'قانون الذكاء الاصطناعي' في نهاية مايو ٢٠٢٤. وقد كان هذا القانون محل اهتمام من مؤسسات الاتحاد الأوروبي منذ أن تقدمت المفوضية الأوروبية بمقترح لتنظيم أنشطة الذكاء الاصطناعي في الاتحاد الأوروبي في ٢١ أبريل ٢٠٢١. واعتمده المجلس الأوروبي رسميًا في ٢١ مايو ٢٠٢٤ بعد سلسلة طويلة من المناقشات والإجراءات.

---

[١] لائحة الاتحاد الأوروبي رقم ١٦٨٩/٢٠٢٤ أو ما يسمى بـ "قانون الذكاء الاصطناعي"، انظر في ذلك:

REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 June 2024, No. 2024/1689, Official Journal of the European Union, 12 July 2024, para. 28, available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj [Accessed: 25 July 2024].

يشار إليه فيما بعد في هذا البحث بقانون الذكاء الاصطناعي، أو (EU AI Act).

وفي ١٢ يوليو ٢٠٢٤، نُشر قانون الذكاء الاصطناعي في الجريدة الرسمية للاتحاد الأوروبي، ودخل حيز التنفيذ في جميع الدول الأعضاء السبع والعشرين في الاتحاد الأوروبي اعتبارًا من ١ أغسطس ٢٠٢٤ وبدأ تطبيق غالبية أحكامه في ٢ أغسطس ٢٠٢٦. على أن تدخل الالتزامات المدرجة في القانون حيز التنفيذ تدريجيًا على مدى جدول زمني لتسري معظم الأحكام بحلول منتصف عام ٢٠٢٧[١].

ويُعَد قانون الذكاء الاصطناعي علامة فارقة في تنظيم الذكاء الاصطناعي العالمي، ويعكس هدف الاتحاد الأوروبي في تمهيد الطريق نحو تعزيز نهج تشريعي شامل لدعم الاستخدام الجدير بالثقة والآمن لأنظمة الذكاء الاصطناعي، ويتبع قانون الذكاء الاصطناعي التشريعات الرقمية الرئيسية الأخرى في الاتحاد الأوروبي، مثل اللائحة العامة لحماية البيانات (GDPR)، وقانون الخدمات الرقمية (DSA)، وقانون الأسواق الرقمية (DMA)، وقانون البيانات، وقانون المرونة السيبرانية (CRA).

ويعتبر قانون الذكاء الاصطناعي للاتحاد الأوروبي هو نتيجة لمفاوضات مُكثَّفة هدفت إلى وضع إطار قانوني متناسق "لتطوير أنظمة الذكاء الاصطناعي وطرحها في السوق وتشغيلها واستخدامها" في دول الاتحاد الأوروبي، ويتألف القانون الجديد من ١٨٠ فقرة و١١٣ مادة، ويتبع نهجًا قائمًا على المخاطر (Risk-based Approach) لتنظيم دورة حياة الأنواع المختلفة من أنظمة الذكاء الاصطناعي بالكامل، وتم تضمين القانون عقوبات تتمثل في

---

[١] انظر في ذلك:
EY, The European Union Artificial Intelligence Act, 12 July 2024, p. 2, available at: https://www.ey.com/content/dam/ey-unified-site/ey-com/en-gl/insights/public-policy/documents/ey-gl-eu-ai-act-07-2024.pdf [Accessed: 25 July 2024].

غرامة مالية قصوَى تصل إلى ٣٥ مليون يورو أو ٧٪ من إجمالي المبيعات السنوية على مستوى العالم، أيهما أعلى وذلك لمواجهة عدم الامتثال لأحكام القانون[١].

وينص القانون على منهجية قوية عند تقدير المخاطر في تناول أنظمة الذكاء الاصطناعي "عالية المخاطر"، والتي تشكل خطورة كبيرة على صحة الأشخاص أو سلامتهم أو حقوقهم الأساسية، حيث يتعين على هذه الأنظمة الامتثال لمجموعة من المتطلبات الإلزامية للذكاء الاصطناعي الجدير بالثقة، واتباع إجراءات تقييم المطابقة قبل طرح هذه الأنظمة في سوق الاتحاد الأوروبي[٢].

كما تضمّن القانون تطوراً مهماً للغاية، حيث حظر طرح أو تشغيل أو استخدام بعض الأنظمة في حالات معينة مثل تلك التي تهدف إلى تشويه السلوك البشري، والتي من المحتمل أن تحدث أضرار جسدية أو نفسية، وتستخدم هذه الأنظمة مكونات خفية لا يستطيع الأفراد إدراكها، أو تستغل نقاط ضعف الأطفال أو الأشخاص بسبب أعمارهم أو عجزهم البدني أو العقلي، على نحو ما سنعرض فيما بعد[٣].

---

[١] انظر في ذلك:

Ibid, p. 16.

[٢] انظر في ذلك:

Lilian Edwards, The EU AI Act proposal. Ada Lovelace Institute, 2022, available at: https://shorturl.at/Uqy65 [Accessed: 25 July 2024].

[٣] انظر في ذلك:

Andy Ramos et al, The first Artificial Intelligence Act is here. Key aspects, June 2024, p. 5, available at: https://shorturl.at/w9WE4 [Accessed: 27 July 2024].

ويفرض القانون التزامات واضحة على مُستخدِمي ومُقدِمي خدمات أنظمة الذكاء الاصطناعي، لضمان السلامة واحترام التشريعات القائمة التي تحمي الحقوق الأساسية طوال دورة حياة أنظمة الذكاء الاصطناعي بالكامل، كما تضمّن القانون تحديد الية تنفيذ وتطبيق القواعد من خلال انشاء نظام حوكمة على مستوى الدول الأعضاء، وآلية تعاون على مستوى الاتحاد مع إنشاء مجلس أوروبي للذكاء الاصطناعي (European Artificial Intelligence Board)، كما تم اقتراح تدابير لدعم الابتكار، وخاصةً من خلال صناديق تنظيم الذكاء الاصطناعي وغيرها من الاجراءات، لتقليل العبء التنظيمي ودعم الشركات الصغيرة والمتوسطة الحجم والشركات الناشئة[١].

وبالتالي، فإن كيفية تناول قانون الذكاء الاصطناعي للتزييف العميق أصبحت مسألة محل دراسة لتحديد التنظيم القانوني لهذه التقنية في ضوء نصوص هذا القانون. يتم ذلك من خلال تحديد القواعد القانونية المطبقة عليها، وكذلك الالتزامات المفروضة على مستخدمي هذه التقنية والعقوبات التي تُطبق في حالة مخالفة هذه الالتزامات. وهذا قد يقدم نموذجًا تشريعيًا للمنظمات الأخرى والتشريعات الوطنية يمكن الاستفادة منه في مواجهة هذه التقنية الحديثة.

[١] انظر في ذلك:

Latham & Watkins, EU AI Act: Navigating a Brave New World, July 2024, pp. 2-3, available at : https://shorturl.at/rSxVn [Accessed: 27 July 2024].

أهمية الدراسة

يمثل قانون الذكاء الاصطناعي للاتحاد الأوروبي إطارًا تنظيميًا محوريًا مُصمَمًا لحكم تطوير ونشر أنظمة الذكاء الاصطناعي في دول الاتحاد الأوروبي. ويتمثل جوهر هذا التشريع في تصنيف أنظمة الذكاء الاصطناعي بناءً على مخاطرها المحتملة، بهدف حماية السلامة العامة والحقوق الأساسية، ويمكن استخدام تقنيات الذكاء الاصطناعي، والتي من أهمها التزييف العميق، لإقناع أشخاص بالانخراط في سلوكيات غير مرغوب فيها، أو خداعهم من خلال دفعهم إلى اتخاذ قرارات بطريقة تقوض وتضعف استقلاليتهم.

وحيث إن طرح تقنية التزييف العميق في السوق أو تشغيلها أو استخدامها قد يؤدي إلى أضرار جسيمة، فإن ذلك يستدعي الحاجة إلى دراسة الإطار القانوني لتنظيم هذه التقنية الذي تبناه الاتحاد الأوروبي في قانون الذكاء الاصطناعي باعتبارها منظمة إقليمية رائدة في هذا السياق مما قد يشكل نموذجاً للمنظمات العالمية والإقليمية الأخرى، وكذلك إطاراً للتشريعات الوطنية عند محاولة التنظيم القانوني لهذه التقنية.

المشكلة البحثية

يعد الذكاء الاصطناعي حاليًا إحدى أهم الأولويات في جداول أعمال الاستراتيجيات والسياسات العامة لمعظم البلدان على المستويين الوطني والدولي. وتركز العديد من المبادرات الإقليمية والوطنية على استخدام تطبيقات الذكاء الاصطناعي من أجل التنمية والنمو الاقتصادي من ناحية، وكذلك على مواجهة التحديات التي يثيرها استخدامه من ناحية أخرى. كما يحتل الذكاء الاصطناعي رأس أولويات جداول أعمال المنظمات العالمية والإقليمية، مثل الأمم المتحدة

ومجموعة السبع (G7) ومجموعة العشرين (G20) واليونسكو ومنظمة التعاون الاقتصادي والتنمية (OECD) والمنظمة العالمية للملكية الفكرية (WIPO) والاتحاد الأوروبي وجامعة الدول العربية والاتحاد الأفريقي وغيرها.

يعتبر التزييف العميق أحد تقنيات الذكاء الاصطناعي التي جذبت انتباه المجتمع الدولي في الفترة الأخيرة نظراً لخطورته. ولذلك، تضمن قانون الذكاء الاصطناعي الصادر عن الاتحاد الأوروبي قواعد تهدف إلى ضمان الاستخدام الآمن لأنظمة الذكاء الاصطناعي داخل الاتحاد بشكل عام، كما تضمن قواعد خاصة بتقنية التزييف العميق بنص صريح. ومع ذلك، هناك بعض القواعد العامة التي تُطبق على أنظمة تستوفي شروطًا معينة، مما يستدعي بحث إمكانية تطبيقها على تقنية التزييف العميق. كما تبنى القانون نهجًا لتصنيف أنظمة الذكاء الاصطناعي بناءً على الخطورة، وأفرد قواعد خاصة ببعض الممارسات أو الأنظمة التي تحتاج إلى تحليل لتحديد القواعد القانونية المطبقة على تقنية التزييف العميق.

أهداف الدراسة

تهدف هذه الدراسة إلى تناول التنظيم القانوني لتقنية التزييف العميق في إطار قانون الذكاء الاصطناعي. وعلى الرغم من أن هذا القانون يُطبَق في دول الاتحاد الأوروبي، إلا أنه من شأن هذه الدراسة أن تقدِم أيضاً نموذجاً للمنظمات الإقليمية العربية والتشريعات الوطنية العربية التي تسعى إلى تنظيم أنشطة الذكاء الاصطناعي.

التساؤلات التي تثيرها الدراسة

تهدف هذه الدراسة إلى الإجابة على تساؤل رئيسي هو: ما هو التنظيم القانوني للتزييف العميق وفقاً لقانون الذكاء الاصطناعي الصادر من الاتحاد الأوروبي؟

وتتطلب الإجابة على هذا التساؤل الرئيسي الإجابة على عدة تساؤلات فرعية هي:

١- ما هو تعريف التزييف العميق وما هي أهم خصائصه؟
٢- ما هي القواعد القانونية المطبقة على التزييف العميق وفقاً لقانون الذكاء الاصطناعي؟
٣- ما هي الالتزامات المفروضة على مقدمي الخدمة أو مستخدمي تقنية التزييف العميق وفقاً لقانون الذكاء الاصطناعي؟ وما هي العقوبات المفروضة في حالة مخالفة هذه الالتزامات؟

منهج الدراسة

تعتمد هذه الدراسة على المنهج التحليلي في تحليل النصوص القانونية الواردة في قانون الذكاء الاصطناعي وبحث مدى وكيفية تطبيقها على أفعال التزييف العميق. كما تعتمد الدراسة على المنهج الوصفي في تناول مفهوم التزييف العميق والتطرق لخصائصه المختلفة والأضرار التي قد يشكلها.

خطة الدراسة

نظراً لأن هذه الدراسة تهدف إلى تناول التنظيم القانوني للتزييف العميق في قانون الذكاء الاصطناعي الصادر من الاتحاد الأوروبي، فسوف نقوم بتقسيم هذه الدراسة إلى مبحثين، نتناول في المبحث الأول ماهية التزييف العميق

وخصائصه، ثم نتناول في المبحث الثاني التنظيم القانوني للتزييف العميق في قانون الذكاء الاصطناعي، وذلك على النحو التالي:

المبحث الأول: ماهية التزييف العميق وخصائصه

المطلب الأول: تعريف التزييف العميق

المطلب الثاني: خصائص التزييف العميق

المبحث الثاني: التنظيم القانوني للتزييف العميق في قانون الذكاء الاصطناعي

المطلب الأول: مدى إمكانية اعتبار التزييف العميق ضمن الممارسات المحظورة

المطلب الثاني: مدى إمكانية اعتبار التزييف العميق ضمن الفئات عالية الخطورة

المطلب الثالث: تطبيق الالتزام بالشفافية والتمييز على التزييف العميق

المبحث الأول

ماهية التزييف العميق وخصائصه

أثار ظهور جيل جديد من الوسائط التي يتم التلاعب بها رقمياً مخاوف كبيرة بشأن إساءة الاستخدام المحتملة لهذه الوسائط. فقد مَكّن التقدم في مجال الذكاء الاصطناعي من إنتاج صور أو مقاطع فيديو أو مقاطع صوتية مزيفة، ولكنها تبدو واقعية للغاية، تصور شخصًا يقول أو يفعل شيئًا لم يقله أو يفعله أبدًا أو تصور شيئاً على غير حقيقته. وفي خلال السنوات الأخيرة، أصبح المصطلح الشائع الذي يستخدم غالبًا لهذه التقنية هو "التزييف العميق"، حيث تُستخدم أحد أنظمة الذكاء الاصطناعي لتزوير المقاطع الصوتية أو الصور أو الفيديوهات.

وبذلك فالتزييف العميق هو أحد تقنيات الذكاء الاصطناعي التي تقوم بدمج الأصوات الفردية وتعبيرات الوجه وحركات الجسم في محتوى زائف بمساعدة تقنية تسمى بـ(الشبكة العصبية) أو (Neural Network)[١]، والتي تجعل من الممكن انشاء محتويات الصوت، أو الصور، أو الفيديو، أو التلاعب بها لتبدو واقعية للغاية وتجعل من الصعب التعرف على أنها مزيفة بحيث يفشل

[١] الشبكة العصبية هي برنامج أو نموذج تعلُّم آلي يتخذ القرارات بطريقة مشابهة للدماغ البشري، وذلك باستخدام العمليات التي تحاكي الطريقة التي تعمل بها الخلايا العصبية البيولوجية معًا لتحديد الظواهر ووزن الخيارات والوصول إلى الاستنتاجات. انظر في ذلك:
Mohaiminul Islam et al, An Overview of Neural Network, American Journal of Neural Networks and Applications, 5(1): 7-11, 2019, p. 7, available at: http://www.sciencepublishinggroup.com/j/ajnna [Accessed in: 25 July 2024].

المستخدمون في تمييز ذلك بالعين المجردة[١]. لذلك، فإن إساءة استخدام تقنية التزييف العميق من شأنها أن تدفع البشر إلى عصر تتلاشى فيه الحقيقة، وتؤدي إلى سلسلة من المخاطر لتعرض الحقوق والمصالح الشخصية المشروعة، والأمن العام، وحتى الأمن الوطني للخطر[٢].

ونظراً للتطور السريع للتكنولوجيا وسهولة استخدام تقنية التزييف العميق، فضلاً عن إتاحتها للجميع وانخفاض تكلفتها، فإن ذلك سيؤدي إلى زيادة نسب الاستخدام السلبي والمستخدمين الضاريين لها[٣]، وهو ما يؤكد أهمية التنظيم القانوني لهذه التقنية، وأول المسائل التي تثيرها دراسة هذه التقنية هي محاولة وضع تعريف محدد لها وتوضيح أهم خصائصها، وهو ما سنتناوله من خلال هذا المبحث من خلال تقسيمه على النحو التالي:

المطلب الأول: تعريف التزييف العميق

المطلب الثاني: خصائص التزييف العميق

---

[١] أحمد محمد الخولى، المسئولية المدنية الناتجة عن الاستخدام غير المشروع لتطبيقات الذكاء الاصطناعي "الديب فيك نموذجاً"، مجلة البحوث الفقهية والقانونية، العدد ٣٦، أكتوبر ٢٠٢١، ص ٢٥٢.

[٢] انظر في ذلك:

Ibid.

[٣] محمد مشعل، الذكاء الاصطناعي وآثاره علي حرية التعبير في مواقع التواصل الاجتماعي، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة المنصورة، المجلد ١١، العدد ٧٧، سبتمبر ٢٠٢١، ص ٥٠٥.

المطلب الأول

تعريف التزييف العميق

ظهر مصطلح التزييف العميق للمرة الأولى للعامة في عام ٢٠١٧[١]، والذي أُعتبِر حينها ظاهرة جديدة وكان موضوعًا للعديد من التحليلات التي ركزت على عدة أمور من بينها الطرق المختلفة التي تُستخدم بها هذه التقنية لإلحاق الضرر. وتشمل المخاطر المحتملة لإساءة استخدام التزييف العميق انتشار الأخبار المزيفة والمعلومات المضللة، والتلاعب بالانتخابات، وإنشاء محتوى إعلامي غير صحيح، والتشهير، وتشويه سمعة الأفراد، بما في ذلك المعارضين السياسيين، والسخرية منهم، وتقويض الثقة في رسائل وسائل الإعلام التقليدية، وتشويه الواقع، وإضعاف المشاركة السياسية داخل المجتمع، والتهديدات لاستقرار الأنظمة الاقتصادية، وانتشار خطاب الكراهية، فضلاً عن الأذى النفسي للأفراد أو الفئات الضعيفة[٢].

---

[١] عندما نشر أحد المستخدمين على موقع (Reddit) مقطع فيديو مزيف يستبدل وجه أحد الأشخاص في مقطع فيديو، كما ظهرت أيضًا بعض مقاطع الفيديو المزيفة عن سياسيين مثل ترامب وأوباما، انظر في ذلك:

Min Liu and Xijin Zhang, Deepfake Technology and Current Legal Status of It, Proceedings of the 2022 3rd International Conference on Artificial Intelligence and Education (IC-ICAIE 2022), 27 December 2022, p. 1309, available at: https://www.atlantis-press.com/proceedings/ic-icaie-22/125981029 [Accessed: 25 July 2024].

[٢] انظر في ذلك:

Maria Pawelec, Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions, Digital Society, vol. 2, no. 2, 2022, p. 10, available at: https://doi.org/10.1007/s44206-022-00010-6 [Accessed: 25 July 2024].

على أن هذا الاستخدام الضار للتزييف العميق لا يؤدي إلى القول بإنكار أي وجود للعديد من التطبيقات الإيجابية له في وسائل الإعلام والتعليم والترفيه والخدمات الطبية، لذلك، فإن التنظيم القانوني لمواجهة العواقب التي قد تنتج من الاستخدام الضار للتزييف العميق يصبح هو الحل الوحيد لمواجهة هذه الأزمة[١].

وعلى الرغم من ذلك لم يصدر، في بداية الأمر، أي قوانين خاصة لتنظيم مسألة التزييف العميق، وكان الأمر متروك للقواعد العامة في القانون المدني والقانون الجنائي أو قوانين الملكية الفكرية، إلا أن منظمة الاتحاد الأوروبي قد أدركت خطورة هذه التقنية وعدم كفاية القواعد العامة لتنظيمها، فكان صدور قانون الذكاء الاصطناعي خطوة جوهرية لتنظيم هذه الظاهرة ليس فقط من خلال الإشارة إليها في القانون، ولكن أيضًا من خلال استخدام أدوات وسلطات منظمة الاتحاد الأوروبي لتطبيق تدابير مضادة أكثر صرامة، حيث إن تطوير التكنولوجيا وإساءة الاستخدام المُبلَغ عنها بشكل متكرر يتطلب تنظيماً

انظر أيضاً:

E. Pashentsev, "The Malicious Use of Deepfakes Against Psychological Security and Political Stability," in The Palgrave Handbook of Malicious Use of AI and Psychological Security, E. Pashentsev, Ed. London: Palgrave Macmillan, Cham, 2023, pp. 47–80, available at: https://shorturl.at/UpTZz [Accessed: 27 July 2024].

[١] انظر في ذلك:

Felix Juefei-Xu et al., Countering Malicious DeepFakes: Survey, Battleground, and Horizon, International Journal of Computer Vision, vol. 130, no. 7, 2022, p. 4, available at: https://arxiv.org/pdf/2103.00218 [Accessed: 27 July 2024].

للتزييف العميق بشكل مباشر، وإذا لزم الأمر، حظره إذا كان ينتهك حقوق الغير بشكل مباشر، على نحو ما سنرى فيما بعد[١].

وعند الحديث عن تعريف مصطلح التزييف العميق، نجد أن المادة الثالثة من قانون الذكاء الاصطناعي أوردت مجموعة من التعريفات التي تتعلق بأنظمة الذكاء الاصطناعي وعرفت الفقرة ٦٠ من هذه المادة مصطلح "التزييف العميق" بأنه "صورة أو محتوى صوتي أو فيديو تم إنشاؤه أو التلاعب به بواسطة الذكاء الاصطناعي بهدف مماثلة أشخاص، أو أشياء، أو أماكن، أو كيانات، أو أحداث معينة، ويظهر –على غير الحقيقة– للشخص العادي أنه أصلي أو صحيح"[٢].

وعلى هذا النحو يمكن استخدام تقنيات التزييف العميق لمجموعة متنوعة من الأغراض قد تكون ذات تأثيرات إيجابية أو سلبية، فيمكن استخدام تقنيات التزييف العميق لتحقيق مجموعة من الفوائد والتي من أهمها:

١– الإنتاجات الرسومية الصوتية (Audio graphic productions): حيث تقدم تقنيات التزييف العميق في المقام الأول العديد من الفوائد لمُنتجي، ومُحرِري الصوت والصور والفيديو. وبذلك يمكن لمنتجي الأفلام على سبيل

---

[١] انظر في ذلك:

Rüya Tuna Toparlak, "Criminalising Pornographic Deep Fakes: A Gender-Specific Inspection of Image-Based Sexual Abuse," SciencesPo Law School The 10th Graduate Conference, 2022, p. 22, Available: https://shorturl.at/y1ie1 [Accessed in: 29 July 2024].

[٢] الفقرة ٦٠ من المادة الثالثة من قانون الذكاء الاصطناعي الصادر من الاتحاد الأوروبي والتي تنص على:

'Deep fake' means AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful.

المثال تعديل الفيديوهات أو الأصوات المنطوقة من خلال الدبلجة الصوتية، وإجراء تغييرات على النصوص دون تكلفة إعادة التسجيل لهذه اللقطات، أو إنشاء نسخ مدبلجة لممثلين يتحدثون لغات مختلفة. وفي المستقبل، يمكن لنجوم السينما حتى استخدام تقنيات التزييف العميق ومشاركة نسختهم الرقمية مع المنتجين، حتى يتمكنوا من إنشاء لقطات جديدة دون الحاجة إلى السفر للتصوير[١].

٢- مؤتمرات الفيديو (Video conferencing): يمكن أن تُستخدَم تقنيات التزييف العميق في مؤتمرات الفيديو أيضًا، وذلك عن طريق إتاحة إمكانية حضور المستخدمين كصور رمزية واقعية في الأحداث الافتراضية، مثل المؤتمرات الافتراضية، أو تحسين جودة مؤتمرات الفيديو العادية[٢].

٣- التطبيقات الطبية (البحثية): هناك تطبيقات مفيدة لتقنية التزييف العميق في المجال البحثي والعلاجات الطبية، وذلك في طب الأسنان وجراحات التجميل على سبيل المثال[٣].

---

[١] انظر في ذلك:

Catherine Kerner and Mathias Risse, 'Beyond Porn and Discreditation: Epistemic Promises and Perils of Deepfake Technology in Digital Lifeworlds,' Moral Philosophy and Politics, November 11, 2020, pp. 82-83, available at: https://doi.org/10.1515/mopp-2020-0024 [Accessed: 29 July 2024].

[٢] انظر في ذلك:

'Facebook Is Building the Future of Connection with Lifelike Avatars,' Facebook Technology, March 13, 2019, available at: https://tech.facebook.com/reality-labs/2019/3/codec-avatars-facebook-reality-labs/ [Accessed: 29 July 2024].

[٣] انظر في ذلك:

Snapshot Paper - Deepfakes and Audiovisual Disinformation, Independent report, 12 September 2019, available at: https://shorturl.at/gQvUV [Accessed: 29 July 2024].

وعلى الجانب الاخر، قد يكون لتقنية التزييف العميق بعض الجوانب السلبية والتي من أشهرها:

١- **الأضرار النفسية (psychological harms)**: فقد يتسبب إنشاء ونشر مقاطع فيديو مزيفة في أضرار نفسية بالغة للشخص الذي يتم تمثيله. كما يمكن استخدام مقاطع الفيديو المزيفة للتنمر والتشهير والترهيب، مما قد يتسبب في أضرار نفسية عميقة. ومن بين العواقب المهمة الأخرى المترتبة على التلاعب بمقاطع الفيديو والصوت لأشخاص يقومون أو يقولون أشياء لم يفعلوها أو يقولوها قط استخدام هذه المقاطع للابتزاز[١]. فمن خلال التهديد بفضح المحتوى الملفق، يكتسب الجناة سلطة على ضحاياهم، على سبيل المثال لمطالبة الضحايا بمبالغ أو اتباع تعليمات معينة[٢].

٢- **الأضرار المالية (financial harms)**: إن استخدام التزييف العميق قد يؤدي أيضًا إلى احداث العديد من الأضرار المالية. فقد تمتد أضرار ممارسات الابتزاز المذكورة أعلاه من مجرد الضرر النفسي إلى الضرر المالي. علاوةً على ذلك، فإن الأفعال الإجرامية مدفوعة في الغالب بدوافع مالية، وقد يلحق هذا الضرر المالي بالأفراد وكذلك المنظمات أو المؤسسات،

---

[١] أحمد محمد البوشي، الابتزاز الإلكتروني مفهوم جديد في جرائم التهديد المعلوماتية: دراسة تفصيلية في ضوء قانون العقوبات وقانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ وأحدث أحكام محكمة النقض المصرية، دار النهضة العربية، ٢٠٢٢، ص ٢٣.

انظر أيضاً:

حسين عبد الكريم، خليل يوسف الجندي، الابتزاز الإلكتروني والجرائم الإلكترونية – المفهوم والأسباب، دار كفاءة المعرفة للنشر والتوزيع، عمان، ٢٠١٩، ص ٥١.

[٢] انظر في ذلك:

Tackling deepfakes in European policy, EPRS | European Parliamentary Research Service, July 2021, p. 30, available at: https://shorturl.at/gSZRw [Accessed: 29 July 2024].

حيث يمكن إفساد الموظفين من خلال الابتزاز. كما يمكن استخدام تقنية التزييف العميق لسرقة الهوية من خلال الحصول على بيانات جوهرية في عملية التحقق من المعاملات المصرفية عبر الإنترنت، أو هوية الموظفين في مؤسسة ما، ويمكن استخدام هذا الشكل الجديد من سرقة الهوية لأغراض مختلفة، مثل إنشاء تقليد مقنع لرؤساء يصدرون الأوامر أو التوجيهات للموظفين. وبذلك يمكن أن يؤدي التزييف العميق أيضًا إلى تمكين العديد من أساليب الاحتيال الأخرى، كتصوير مقطع فيديو مزيف يحرض على الكراهية أو الإهانات أو أي سلوك غير أخلاقي أو غير قانوني آخر[١].

٣- **الأضرار المجتمعية (societal harms):** تشكل فئة المخاطر هذه مستودعًا للتأثيرات السلبية المحتملة لتقنيات التزييف العميق في قطاعات ومؤسسات مجتمعية متعددة، وتشمل القطاعات المجتمعية المعرضة للخطر تلك التي تعتمد بشكل كبير على الأدلة الموثقة، مثل التأمين والصحافة والإعلام والتعليم، والأنظمة المجتمعية والاقتصادية مثل السوق المالية ونظام العدالة الجنائية والأنظمة السياسية والعلمية. فغالبًا ما ترتبط مخاطر التزييف العميق بالأضرار المحتملة الناجمة عن التضليل أو الخداع بهدف التأثير على الرأي العام، أو جمع تبرعات وهمية، أو تشويه سمعة الشخصيات العامة[٢].

---

[١] انظر في ذلك:

Vincenzo Ciancaglini et al., Malicious Uses and Abuses of Artificial Intelligence, Trend Micro Research, 2020, p. 31, available at: https://documents.trendmicro.com/assets/white_papers/wp-malicious-uses-and-abuses-of-artificial-intelligence.pdf [Accessed: 29 July 2024].

[٢] انظر في ذلك:

Tom Dobber et al., 'Do (Microtargeted) Deepfakes Have Real Effects on Political Attitudes?,' The International Journal of Press/Politics,

كما أنه من الممكن أن تلحق تقنية التزييف العميق الضرر بالعملية الديمقراطية بعدة طرق، وخاصة المناظرات العامة والانتخابات وشرعية المؤسسات الديمقراطية وسمعة السياسيين[١].

كما إن وسائل الإعلام التي يتم التلاعب بها ونشر معلومات مزيفة من شأنها أن تلحق الضرر بالاستقرار الاقتصادي. على سبيل المثال، يمكن أن يكون للتصريحات المصطنعة حول النزاع بين دولتين تأثير سلبي على سعر السلع الحيوية مثل النفط وبالتالي على الاقتصاد العالمي[٢].

كما قد تلحق تقنية التزييف العميقة الضرر أيضًا بأنظمة العدالة، ويمكن استخدام مقاطع الفيديو المزيفة واستنساخ الأصوات والصور والفيديوهات الاصطناعية لإنشاء أدلة كاذبة أو التلاعب بها أمام المحاكم. وبالتالي، يثير التزييف العميق مخاوف جدية بشأن مصداقية وقبول المحتويات السمعية والبصرية كدليل إلكتروني أمام المحاكم، وحتى عندما تكون إجراءات التحقق الحالية من الأدلة الصوتية والفيديو قادرة على اكتشاف

July 25, 2020, p. 70, available at: https://journals.sagepub.com/doi/10.1177/1940161220944364 [Accessed: 29 July 2024].

[١] انظر في ذلك:

W Lance Bennett and Steven Livingston, 'The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions,' European Journal of Communication 33, no. 2, 1 April 2018, 122–39, p. 127, available at: https://journals.sagepub.com/doi/10.1177/0267323118760317 [Accessed: 29 July 2024].

[٢] انظر في ذلك:

Jon Bateman, Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios, Carnegie Endowment for International Peace, July 2020, p. 22, available at: https://shorturl.at/IlgU0 [Accessed: 29 July 2024].

التزييف العميق، فإن وجود التزييف العميق قد يؤثر على الشهادات، لأن الناس قد يشهدون بناءً على ما رأوه أو سمعوه من المحتويات المزيفة خارج المحكمة. وبذلك قد يؤدي التزييف العميق إلى قلق أوسع نطاقًا بشأن ضياع الثقة في المجتمع بشكل عام نتيجة لأن المعلومات الموجودة لم تعد جديرة بالثقة[١].

٤- **الإضرار بالأمن القومي والعلاقات الدولية:** قد تؤدي تقنية التزييف العميق أيضًا إلى تفاقم الانقسامات الاجتماعية والاضطرابات المدنية والذعر والصراعات وتقويض السلامة العامة والأمن القومي[٢]، والذي قد يتسبب في صراعات عنيفة وهجمات على السياسيين وانهيار الحكم أو تهديدات للعلاقات الدولية. فعلى سبيل المثال في عام ٢٠١٨، تم نشر مقطع فيديو عن (علي بونغو أونديبا)، رئيس الجابون، على الإنترنت يبدو مشوشاً بعض الشيء، وأصبح الاعتقاد السائد، بإعلان المعارضة، أنه في حالة صحية سيئة، أو حتى ميتًا. وهو ما أدى إلى أزمة وطنية ومحاولة فاشلة للانقلاب عليه[٣].

---

[١] انظر في ذلك:

Regina Rini, Deepfakes and the Epistemic Backstop, Philosopher's Imprint 20, no. 24, 2020, pp. 2-4, available at: https://philpapers.org/archive/RINDAT.pdf [Accessed: 29 July 2024]

[٢] انظر في ذلك:

Danielle K. Citron and Robert Chesney, Deep Fakes: A Looming Challenge for Priv es: A Looming Challenge for Privacy, Democr , Democracy, and National Security, California Law Review, 2019, p. 1758, available at: https://scholarship.law.bu.edu/faculty_scholarship/640 [Accessed: 29 July 2024]

[٣] انظر في ذلك:

ولما كان الدولة هي سبب وجود القانون الدولي العام والشرط اللازم لاستمراره وتطوره، فبالتالي كان من اللازم أن يتدخل لمواجهة ما قد يؤدي إلى تهديد بقاءها والتأثر على أمنها واستقرارها[١]. وقد يؤدي استخدام التزيف العميق إلى الإضرار بسلامة الدول وأمنها من ناحية، والتأثير على علاقتها الخاجية في المجتمع الدولي.

ومن أمثلة النزاعات الدولية التي استخدمته فيها تقنية التزييف العميق مؤخراً ما حدث في الثاني من مارس ٢٠٢٢، بعد وقت قصير من الغزو الروسي لأوكرانيا، حيث تم نشر مقطع فيديو للرئيس الأوكراني (فولوديمير زيلينسكي) وهو يقف على المنصة ويطلب من مواطنيه الأوكرانيين إلقاء أسلحتهم والاستسلام لروسيا. وأشار المستخدمون إلى التناقضات في الفيديو، من تشوه الصورة إلى اختلاف لون بشرة الرئيس بين وجهه ورقبته. والواقع أن هذا الفيديو لم يكن تصريحا حقيقيا من الرئيس الأوكراني، بل كان في واقع الأمر تزييفا عميقا[٢].

وعلى ذلك، يمكن للدول والفاعلين من غير الدول، استخدام تقنية التزييف العميق لتحقيق أغراض متعددة، ومنها على سبيل المثال:

Sarah Cahlan, 'How Misinformation Helped Spark an Attempted Coup in Gabon, Washington Post, 2020, available at: https://shorturl.at/05j9k [Accessed: 29 July 2024]

[١] أ.د/ محمد صافي يوسف، تدابير حماية الأمن القومي كاستثناء على تطبيق قواعد القانون الدولي العام، المجلة المصرية للقانون الدولي، ٢٠١٠، ص ١٧١.

[٢] انظر في ذلك:

James Pearson and Natalia Zinets, "Deepfake Footage Purports to Show Ukrainian President Capitulating," Reuters, 17 March 2022, available at: https://shorturl.at/ZFI6X [Accessed: 29 July 2024]

أولاً: إضفاء الشرعية على الحرب والانتفاضات:

لطالما استخدمت الدول المعلومات الكاذبة وتظاهرت بالغضب والانتقام كذرائع للحرب. فعلى سبيل المثال، قبل غزو ألمانيا لبولندا في عام ١٩٣٩، استولى ضباط من قوات الأمن الخاصة الألمانية، يرتدون الزي البولندي، على محطة إذاعية وبثوا رسالة تدين ألمانيا لتبرير الغزو الألماني[١]. وحيث أنه يمكن استخدام مقاطع الفيديو والصوت لإثبات وقائع معينة عن نية الغزو أو خلافه، فإن تزييف هذه المقاطع قد يؤدي إلى بدء الصراعات الدولية أو تأجيجها في حالات أخرى.

ثانياً: تزييف أوامر القادة أثناء النزاعات:

فيمكن باستخدام تقنية التزييف العميق إنشاء محتوى صوتي ومرئي وتصويره على أنه صادر من القادة. وهو ما حدث بالفعل في مقطع الفيديو الروسي للرئيس الأوكراني، حيث يظهر وهو يأمر الجنود الأوكرانيين بإلقاء أسلحتهم والاستسلام للقوات الروسية الغازية. وقد تتضمن بعض الأوامر الزائفة مقاطع فيديو لقادة كبار يطلبون من الجنود إلقاء أسلحتهم والانسحاب، وتشجيع الاستسلام الجماعي، والتحرك الخاطئ للقوات المحمية بصورة جيدة، مما يجعل هذه القوات عرضة للخطر[٢].

---

[١] انظر في ذلك:

CHRISTOPHER KLEIN, How Germany's Invasion of Poland Kicked Off WWII, History, 2014, available at: https://shorturl.at/3JavJ [Accessed: 29 July 2024]

[٢] انظر في ذلك:

Greg Allen and Taniel Chan, Artificial Intelligence and National Security, Cambridge: Belfer Center for Science and International Affairs, July 2017, available at: https://shorturl.at/IDMtV [Accessed: 29 July 2024]

ومن شأن ذلك أيضاً أن يخلق حالة من الارتباك، مما قد يؤدي إليه من توجيه المدنيين والجنود لتجاهل تعليمات القادة باعتبارها مزيفة. فقد يتجاهلون عن غير قصد الأوامر الصحيحة خوفاً من كونها أوامر أو تعليمات مزيفة. كما يمكن أيضًا زرع الارتباك على المستوى التكتيكي أثناء الصراع؛ فمن الممكن استخدام التزييف العميق لإظهار صورة لجنود أعداء يدخلون مدينة أو يرفعون علمًا في مدينة محتلة. وقد يؤدي هذا إلى اعتقاد الجنود المدافعين بأنهم في خطر وشيك، وبالتالي يدفعهم إلى الفرار من أرض المعركة[١].

وقد يؤدي ذلك أيضاً إلى شق الصفوف بين القوات، فعادة ما تقاتل الجيوش المنقسمة بشكل سيئ. ونتيجة لذلك، فإن الحفاظ على تماسك الوحدة وروح الفريق يشكل جزءًا مهمًا من التدريب والقيادة. ويمكن للخصم إنشاء محتوى يُظهر كبار القادة السياسيين أو العسكريين وهم يدلون بتصريحات عنصرية، ويعبرون عن ازدرائهم لجنودهم ورؤسائهم السياسيين، ويسخرون من القتلى أو الجرحى، أو يشوهون سمعتهم بطرق أخرى. وبذلك، قد تُظهر أيضًا مثل هذه الاستخدامات لتقنية التزييف العميق القادة العسكريين وهم يشككون في سلطة رؤسائهم أو يصفون معركة أو حربًا جارية بأنها اقتراح خاسر، مما يؤدي إلى نقص الإرادة للقتال بين الجنود[٢].

---

[١] انظر في ذلك:

Henry Farrell, Abraham Newman, and Jeremy Wallace, Spirals of Delusion, Foreign Affairs, September/October 2022, available at: https://www.foreignaffairs.com/world/spirals-delusion-artificial-intelligence-decision-making [Accessed: 29 July 2024]

[٢] انظر في ذلك:

Jason Lyall, Divided Armies: Inequality and Battlefield Performance in Modern War, Princeton University Press, 2020, p. 575, available at: https://academic.oup.com/ia/article/97/2/573/6159415 [Accessed: 29 July 2024]

ثالثاً: تقويض الدعم الشعبي:

ففي الحروب، لا تقاتل الجيوش بمفردها. فهي تحتاج إلى مجندين ودعم مالي، وربما الأهم من ذلك، معنويات عالية؛ فهي تريد أن يُنظر إليها على أنها تقاتل من أجل شيء ما. بالنسبة للمتمردين، فإن الدعم الشعبي أمر حيوي أيضًا لضمان حصولهم على طعام كافٍ وممر آمن للهروب من القوات الحكومية المتفوقة عسكريًا. قد تُظهر عمليات التزييف العميق القوات العسكرية وهي ترتكب انتهاكات لحقوق الإنسان، أو تنحاز لجماعة معينة على حساب جماعة أخرى، أو تفر كجبناء بدلاً من القتال بشجاعة، أو تنهب وتسرق من المجتمع المحلي، مما يؤدي إلى تقويض الدعم الشعبي للقوات وخسارة واحد من أهم عناصر الدعم أثناء النزاعات. ومن شأن ذلك أيضاً أن يؤدي إلى زيادة الانقسامات داخل المؤسسة العسكرية ويؤثر على الثقة في القادة السياسيين[١].

ومن الممكن أن يؤدي التزييف العميق أيضاً إلى انقسام المجتمعات. فقد حاولت روسيا بالفعل استخدام الأخبار المزيفة لاستقطاب المجتمع الأمريكي، وإثارة التوتر بشأن مسيرات حماية السود (Black Lives Matter) وغيرها من الاحتجاجات. ويمكن استخدام التزييف العميق لزيادة التوتر من خلال إظهار ضباط الشرطة البيض وهم يصرخون بعبارات عنصرية بينما يطلقون النار على رجال سود عزل أو غير ذلك لإثارة الفتن والنزاعات الداخلية[٢].

---

[١] اسلام دسوقي عبد النبي، دور تقنيات الذكاء الإصطناعى فى العلاقات الدولية والمسئولية الدولية عن استخداماتها، المجلة القانونية، ٢٠٢٠، ص ١٤٥٨.

[٢] انظر في ذلك:

Robert Chesney and Danielle Citron, "Deepfakes: A Looming Crisis for National Security, Democracy and Privacy?", Lawfare, 2018, available at: https://shorturl.at/1czIH [Accessed: 29 July 2024]

كما قد تكون من العواقب التي تنتج عن نشر أخبار زائفة، أن تؤدي إلى انقسام الحلفاء. فلدى الحلفاء أولويات أمنية ومخاوف سياسية محلية مختلفة، ويمكن للمحتوى الكاذب أن يستغل مثل هذه الاختلافات. على سبيل المثال، خلال الحرب الباردة، تم تسريب تقارير رسمية أمريكية مزيفة، دعت إلى استخدام الأسلحة النووية على أراضي دول أعضاء في منظمة حلف شمال الأطلسي (NATO)، مما أثار غضبًا واسع النطاق. كما يمكن أن تقدم تقنية التزييف العميق طريقة مقنعة لإظهار القادة وهم يدلون بتعليقات ازدرائية وغير مبالية بشأن الحلفاء أو الضحايا؛ والتعامل غير الصحيح مع قضايا حساسة لدول حليفة (على سبيل المثال، تدفق اللاجئين أو نقص الطاقة)؛ أو التصرف بطرق أخرى من شأنها أن تضعف علاقة ثنائية أو متعددة الأطراف[١].

كما يمكن استخدام مقاطع الفيديو المزيفة لتشويه سمعة القادة. فقد تم استخدام مقطع فيديو مزيف في ميانمار لإظهار وزير سابق في الحكومة يقول إنه رشى زعيمة البلاد السابقة (أونج سان سو كي)[٢]. وفي بداية الأمر، كان الخطر الأعظم من الدول التي تتمتع بقدرة تكنولوجية كبيرة أو يمكنها توظيفها، ولكن مع تطور التكنولوجيا وزيادة إمكانية الوصول إليها، بدأت الدول النامية والجهات الفاعلة غير الحكومية وحتى الأفراد في استخدام تقنية التزييف العميق.

---

[١] انظر في ذلك:
Thomas Rid, Active Measures: The Secret History of Disinformation and Political Warfare, Volume 64, No. 1, March 2020, pp. 120-128, available at: https://shorturl.at/YzdK8 [Accessed: 29 July 2024]

[٢] انظر في ذلك:
Tom Simonite, "A Zelensky Deepfake Was Quickly Defeated. The Next One Might Not Be," WIRED, 17 March 2022, available at: https://shorturl.at/lcFoi [Accessed: 29 July 2024]

تشير كل هذه الأمثلة والاستخدامات إلى أهمية وزيادة استخدام تقنية التزييف العميق. وهذا ما يؤكده أيضاً ما ورد في المنتدى الاقتصادي العالمي، حيث ارتفعت مقاطع الفيديو المزيفة بمعدل يزيد عن ٩٠٠٪ سنوياً. وبحسب تقديرات إحدى الشركات الناشئة، قفز عدد مقاطع الفيديو المزيفة على الإنترنت من ١٤٦٧٨ مقطعًا في عام ٢٠١٩ إلى ١٤٥٢٧٧ مقطعًا بحلول يونيو من العام التالي[١]. وفي جميع أنحاء العالم، هناك مخاوف من أن تصبح التكنولوجيا بشكل متزايد مصدرًا للتضليل، والانقسام، والاحتيال، والابتزاز[٢].

وقد توقع خبراء الذكاء الاصطناعي ومستشاري السياسات أنه بسبب النمو الهائل في تبني الذكاء الاصطناعي، من المرجح أن يتم انتاج ٩٠٪ من محتوى الإنترنت بالكامل بواسطة الذكاء الاصطناعي في عام ٢٠٢٥[٣]، وحتى لو لم تبلغ نسبة المواد المنتجة بواسطة الذكاء الاصطناعي ٩٠٪ بحلول العام

---

[١] انظر في ذلك:

How to tell reality from a deepfake?, World Economic Forum, April 2021, available at: https://shorturl.at/swCiu [Accessed: 29 July 2024]

[٢] هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، دار النهضة العربية، ٢٠٠٦، ص ٢٥.

انظر أيضاً:

د. حسام محمد السيد محمد، المواجهة الجنائية لظاهرة الثأر الإباحي دراسة مقارنة بين النظامين الأنجلو أمريكي واللاتيني الجزء الثاني، مجلة الدراسات القانونية والاقتصادية، المجلد ٥، العدد ٢، ديسمبر ٢٠١٩، ص ٥١، متاح على: https://shorturl.at/6jhKl

[٣] انظر في ذلك:

Tor Constantino, Is AI quietly killing itself – and the Internet?, Forbes, 2024, available at: https://shorturl.at/e6nKM [Accessed: 29 July 2024]

المقبل، فستظل نسبة كبيرة للغاية توضح أهمية حماية المحتويات المتاحة على الانترنت وخطورة التزييف العميق.

المطلب الثاني

خصائص التزييف العميق

يمكننا أن نستنتج من التعريف الذي أورده قانون الذكاء الاصطناعي للتزييف العميق، بأنه "صورة أو محتوى صوتي أو فيديو تم إنشاؤه أو التلاعب به بواسطة الذكاء الاصطناعي بهدف مماثلة أشخاص، أو أشياء، أو أماكن، أو كيانات، أو أحداث معينة، ويظهر – على غير الحقيقة – للشخص العادي أنه أصلي أو صحيح"، أنه يتسم بمجموعة من الخصائص الهامة التي تميزه كأحد أهم تقنيات الذكاء الاصطناعي في العصر الحالي، وهي على النحو التالي:

أولاً: الطبيعة التقنية، والتي تتعلق بطريقة الإنشاء أو التلاعب بالمحتوى والتي تتم باستخدام التزييف العميق كأحد أنظمة الذكاء الاصطناعي. ويشير مصطلح أنظمة الذكاء الاصطناعي إلى مجموعة من الأساليب والخوارزميات المستخدمة لتطوير أنظمة ذكية يمكنها أداء مهام تتطلب ذكاءً شبيهًا بالذكاء البشري[١]، ومن بين الأساليب المستخدمة على نطاق واسع: التعلم

---

[١] خالد ممدوح إبراهيم، التنظيم القانون للذكاء الاصطناعي، دار الفكر الجامعي، الإسكندرية، ٢٠٢٢، ص ٣٢.

انظر أيضاً:

أحمد مصطفى معوض، استخدامات الذّكاء الاصطناعي استخدام تقنية التزيِيف العميق في قذف الغير نموذجًا دراسة فقهية مقارنة معاصرة، مجلة البحوث الفقهية والقانونية، العدد ٣٩، أكتوبر ٢٠٢٢، ص ٢٥١٢، متاح على:

https://jlr.journals.ekb.eg/article_266108.html

الآلي[١](Machine Learning)، معالجة اللغات الطبيعية[٢](Natural Language Processing)، الرؤية الحاسوبية[٣](ComputerVision)،

[١] التعلم الآلي (ML) هو أحد أهم تقنيات الذكاء الاصطناعي (AI) وعلوم الكمبيوتر والذي يركز على استخدام البيانات والخوارزميات لتمكين الآلات والأجهزة من تقليد الطريقة التي يتعلم بها البشر، وتحسين دقتها تدريجيًا. انظر في ذلك:

Steve Blank, Artificial Intelligence/ Machine Learning Explained, Gordian Knot Center for National Security Innovation, 12 May 2022, available at: https://shorturl.at/XcmFO [Accessed: 29 July 2024].

[٢] يقصد بـ(معالجة اللغة الطبيعية) برمجة أجهزة الكمبيوتر لمعالجة اللغات البشرية لتسهيل التفاعلات بين البشر وأجهزة الكمبيوتر. انظر في ذلك:

Prativa Barik, An Overview of AI Techniques and Their Applications, Journal of Nonlinear Analysis and Optimization Vol. 11, Issue. 1, 2020, available at: https://shorturl.at/a7wQW [Accessed: 29 July 2024].

[٣] يقصد بـ(الرؤية الحاسوبية) التقنية التي تمكن الآلات من القدرة على تفسير المعلومات المرئية من العالم، فباستخدام الرؤية الحاسوبية، يستطيع الكمبيوتر فهم الصور تمامًا مثل ما يفهمها العنصر البشري وقد أحدثت هذه التقنية ثورة في صناعات مثل الرعاية الصحية والسيارات والروبوتات، مما مكن من أداء مهام مثل التعرف على الوجه، واكتشاف الأشياء، والقيادة الذاتية. انظر في ذلك:

Sathesh Sriskandarajah, Computer Vision Fundamentals for Business Leaders PricewaterhouseCoopers, April 2020, p. 5, available at: https://www.pwc.com.au/consulting/assets/pwc-computer-vision-fundamentals-for-business-leaders.pdf [Accessed: 29 July 2024].

التعلم العميق[١](Deep Learning)، استخراج البيانات[٢](Data Mining)، الروبوتات[٣] (Robotics).

ويشير الذكاء الاصطناعي كذلك إلى "محاولة جعل الكمبيوتر أو الالة التي تعمل بالبرمجة مثل الإنسان سواء في تفكيره أو تصرفاته، أو حله لمشكلاته،

---

[١] يعتبر التعلم العميق هو أحد فروع التعلم الآلي والذي يعتمد على بنية الشبكة العصبية الاصطناعية، وهو أسلوب في الذكاء الاصطناعي يعلم أجهزة الكمبيوتر معالجة البيانات بطريقة مستوحاة من الدماغ البشري. انظر في ذلك:

Ranjan Mishra et al, The Understanding of Deep Learning: A Comprehensive Review, Mathematical Problems in Engineering, 5 April 2021, p. 1, available at: https://onlinelibrary.wiley.com/doi/10.1155/2021/5548884 [Accessed: 29 July 2024].

انظر أيضاً:

أشرف سيد أبوالعلا، المواجهة الجنائية لتقنية الديب فيك، مجلة العلوم القانونية والاقتصادية، يناير ٢٠٢٤، ص ٤٨٨، متاح على:

https://jelc.journals.ekb.eg/article_342112.html

[٢] (استخراج البيانات) هي عملية استخراج المعرفة أو الأفكار من كميات كبيرة من البيانات باستخدام تقنيات إحصائية وحسابية مختلفة. يمكن أن تكون البيانات مهيكلة أو شبه مهيكلة أو غير مهيكلة، ويمكن تخزينها في أشكال مختلفة مثل قواعد البيانات ومستودعات البيانات وبحيرات البيانات. انظر في ذلك:

Matthew N. O. Sadiku, DATA MINING: A BRIEF INTRODUCTION, European Scientific Journal, vol.11, No.21, July 2015, p. 509, available at: https://core.ac.uk/download/pdf/328025049.pdf [Accessed: 29 July 2024].

[٣] انظر في ذلك:

عمرو طه بدوي محمد، النظام القانوني للروبوتات الذكية المزودة بتقنية الذكاء الاصطناعي (الإمارات العربية المتحدة كنموذج) دراسة تحليلية مقارنة لقواعد القانون المدني للروبوتات الصادرة عن الاتحاد الأوروبي سنة ٢٠١٧ ومشروع ميثاق أخلاقيات الروبوت الكوري، مجلة الدراسات القانونية والاقتصادية، ٢٠٢١، المجلد ٧، العدد ٢، ص ٨٦١.

وممارسته لكافة نواحي الحياة اليومية، وذلك عن طريق دراسات تجرى على الإنسان، وتستخلص منها نتائج تساعد على تفسير سلوك الإنسان وبرمجة ذلك لتطبيقه على الالة"[١].

وقد أشارت الفقرة ١٢ من ديباجة قانون الذكاء الاصطناعي إلى أنه يجب أن يكون مفهوم "نظام الذكاء الاصطناعي" في هذه اللائحة محددًا بوضوح ويجب أن يتماشى بشكل وثيق مع عمل المنظمات الدولية العاملة في مجال الذكاء الاصطناعي لضمان اليقين القانوني وتسهيل التقارب الدولي والقبول الواسع، مع توفير المرونة لاستيعاب التطورات التكنولوجية السريعة في هذا المجال[٢].

كما تضمنت الفقرة الأولى من المادة الثالثة تعريفاً لنظام الذكاء الاصطناعي، حيث نصت على أن "نظام الذكاء الاصطناعي يعني نظامًا قائمًا على الآلة، مصممًا للعمل بمستويات متفاوتة من الاستقلالية، وقد يُظهر القدرة على التكيف بعد التشغيل، والذي يستنتج، لأغراض صريحة أو ضمنية، من المدخلات التي يتلقاها، كيفية إنشاء مخرجات مثل التنبؤات، أو المحتوى، أو التوصيات، أو القرارات التي يمكن أن تؤثر على البيئات المادية أو الافتراضية"[٣].

---

[١] يحي إبراهيم دهشان، المسئولية الجنائية عن جرائم الذكاء الاصطناعي، مجلة الشريعة والقانون، جامعة الإمارات، ٢٠١٩، ص ١٤.

[٢] انظر في ذلك:

Paragraph 12 of the recitals of the EU AI Act.

[٣] انظر في ذلك:

Paragraph 1 of Article 3 of the EU AI Act. It provides that "'AI system' means a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after

وبذلك، يستند تعريف أنظمة الذكاء الاصطناعي إلى مجموعة من الخصائص الرئيسية التي تميزها عن أنظمة البرمجيات التقليدية الأكثر بساطة، والتي من أهمها قدرتها على الاستنتاج. وتشير هذه القدرة إلى عملية الحصول على مخرجات يمكن أن تؤثر على البيئات المادية والافتراضية، وعلى قدرة أنظمة الذكاء الاصطناعي على استنباط نماذج أو خوارزميات، أو كليهما، من المدخلات أو البيانات[١].

وبالتالي، فإن القول بوقوع فعل التزييف العميق يستند إلى استخدامه كأحد أنظمة الذكاء الاصطناعي. فهو نظام يستخدم تقنيات التعلم العميق والذكاء الاصطناعي لتوليد معلومات رقمية مزيفة أو مُعالجة بشكل مقنع للغاية، في شكل مقاطع فيديو أو صور أو تسجيلات صوتية. وهذا يمثل تحديًا كبيرًا للأفراد الذين يحاولون التمييز بين المحتوى المُعالج والوسائط الأصلية غير المعدلة[٢].

ثانياً: الطبيعة النمطية، والتي تتعلق بشكل الوسائط المستخدمة، فقد حدّدت الفقرة ٦٠ من المادة الثالثة أنه قد يكون المحتوى المزيف عبارة عن صورة أو محتوى صوتي أو فيديو؛ ويمكن القول إن هذا التعريف يشابه إلى حد كبير التعريفات الصادرة من بعض المؤسسات والجهات والتي ذكرت صراحةً أن محتوى التزييف العميق يكون مقطعاً صوتياً أو صورة أو فيديو، بما في ذلك التقارير الصادرة عن وكالة الأمن السيبراني التابعة للاتحاد الأوروبي

---

deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments".

[١] انظر في ذلك:

Ibid.

[٢] انظر في ذلك:

Ruchi Bisht, What is Deepfake AI?, InfosecTrain, November 2023, available at: https://www.infosectrain.com/blog/what-is-deepfake-ai/

(ENISA)[١]، ووكالة الاتحاد الأوروبي للتعاون في مجال إنفاذ القانون (EUROPOL)[٢]، وحلف شمال الأطلسي (NATO)[٣]، وقائمة مصطلحات الذكاء الاصطناعي التي أعدتها مؤسسة (Brookings)[٤].

وعلى الرغم من دعوة بعض الباحثين[٥] إلى ادراج حالة الانشاء أو التلاعب التي قد تقع على (النصوص الكتابية) ضمن حالات التزييف العميق

---

[١] انظر في ذلك:
R. Mattioli, A. Malatras, Identifying Emerging Cyber Security Threats and Challenges for 2030. Athens: ENISA, 2023, p. 31, available at: https://shorturl.at/Ne7aU [Accessed: 10 August 2024]

[٢] انظر في ذلك:
B. van der Sloot, Y. Wagensveld, "Deepfakes: regulatory challenges for the synthetic society," Computer Law & Security Review, vol. 46, 2022, p. 1, available at: https://www.sciencedirect.com/science/article/pii/S0267364922000632?ref=pdf_download&fr=RR-2&rr=8b5e4ddfdb230fe6 [Accessed: 10 August 2024].

[٣] انظر في ذلك:
K. Giles, K. Hartmann, M. Mustaffa, The Role of Deepfakes in Malign Influence Campaigns. Riga: NATO Strategic Communications Centre of Excellence, 2019, p. 8, available at: https://stratcomcoe.org/pdfjs/?file=/publications/download/web_deep_fakes_report_11-08-2019.pdf?zoom=page-fit [Accessed: 10 August 2024].

[٤] انظر في ذلك:
John R. Allen and Darrell M. West, The Brookings glossary of AI and emerging technologies Commentary, The Brookings, 13 July 2020, available at: https://www.brookings.edu/articles/the-brookings-glossary-of-ai-and-emerging-technologies/ [Accessed: 10 August 2024].

[٥] انظر في ذلك على سبيل المثال:
Federal Trade Commission, Combatting Online Harms Through Innovation, Federal Trade Commission Report to Congress, 2022, p. 17, available at: https://shorturl.at/R8k2n [Accessed: 13 August 2024].
انظر أيضاً:

إلا أنه من الواضح أن المادة الثالثة لم تقر ذلك، فاعتبرت التزييف العميق ينصب فقط على الصور أو المقطع الصوتي أو الفيديو.

كما أن القانون قد ميز ذلك بشكل خاص في المادة ٥٠ المتعلقة بالتزامات الشفافية لمقدمي ومستخدمي أنظمة معينة من أنظمة الذكاء الاصطناعي بنصه في الفقرة الرابعة على أنه "...٤- يتعين على مستخدمي نظام الذكاء الاصطناعي الذين يُنشئ أو يتلاعب بمحتوى الصور أو الصوت أو الفيديو الذي يشكل تزييفًا عميقًا، أن يكشفوا أن المحتوى قد تم إنشاؤه أو التلاعب به بشكل مصطنع. ولا ينطبق هذا الالتزام عندما يكون الاستخدام مصرحًا به بموجب القانون للكشف عن جريمة جنائية أو منعها أو التحقيق فيها أو مقاضاة مرتكبيها ..." وأضافت أنه "يتعين على مُستخدِمي نظام الذكاء الاصطناعي الذي يُنشئ أو يتلاعب بنص منشور بغرض إعلام الجمهور بشأن مسائل ذات مصلحة عامة أن يكشفوا أن النص قد تم إنشاؤه أو التلاعب به بشكل مصطنع. لا ينطبق هذا الالتزام في حالة السماح بالاستخدام بموجب القانون للكشف عن الجرائم الجنائية أو منعها أو التحقيق فيها أو مقاضاة مرتكبيها أو في حالة خضوع المحتوى الذي تم إنشاؤه بواسطة الذكاء الاصطناعي لعملية مراجعة بشرية أو مراقبة تحريرية وحيث يتحمل شخص طبيعي أو اعتباري المسؤولية التحريرية عن نشر المحتوى"[١].

Josh A. Goldstein et al., Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations. 2023, p. 7, available at: https://arxiv.org/abs/2301.04246 [Accessed: 13 August 2024]

[١] انظر في ذلك:

الفقرة ٤ من المادة ٥٠ من قانون الذكاء الاصطناعي، والتي تنص على:

فنجد أن الفقرة المذكورة قد ميّزت بين الانشاء أو التلاعب الذي قد يقع على الصور أو الصوت أو الفيديو من جهة والذي قد يقع على نص من جهة أخرى، وأوردت حكماً مختلفاً لكل منهما، وقررت أنه في الحالة الأولى فقط يعتبر ذلك تزييفاً عميقاً أما ما قد يقع على النص لا يعتبر من قبل التزييف العميق بالمفهوم المخالف للنص.

كما تبنت بعض الدراسات نفس النهج عند تعريف التزييف العميق، فعلى سبيل المثال قسّم دليل التزييف العميق الصادر من البرنامج الوطني الإماراتي للذكاء الاصطناعي أنواع المحتوى المزيف إلى فئتين هما:

أولاً: المحتوى المرئي والذي يشمل التزييف العميق الذي يقع على الصور ومقاطع الفيديو، والذي يتم فيه انشاء أو التلاعب بمحتوى معين باستخدام ما يسمى بـ "خوارزميات التشفير" لتبديل وجه شخص مكان وجه شخص اخر على

"Deployers of an AI system that generates or manipulates image, audio or video content constituting a deep fake, shall disclose that the content has been artificially generated or manipulated. This obligation shall not apply where the use is authorised by law to detect, prevent, investigate or prosecute criminal offence. Where the content forms part of an evidently artistic, creative, satirical, fictional or analogous work or programme, the transparency obligations set out in this paragraph are limited to disclosure of the existence of such generated or manipulated content in an appropriate manner that does not hamper the display or enjoyment of the work. Deployers of an AI system that generates or manipulates text which is published with the purpose of informing the public on matters of public interest shall disclose that the text has been artificially generated or manipulated. This obligation shall not apply where the use is authorised by law to detect, prevent, investigate or prosecute criminal offences or where the AI-generated content has undergone a process of human review or editorial control and where a natural or legal person holds editorial responsibility for the publication of the content."

سبيل المثال، أو التلاعب ببعض مكونات الصورة أو الفيديو لتغيير محتواه الأصلي.

ثانياً: المحتوى الصوتي ويشمل انشاء أو تعديل ملف صوتي يتضمن حديثاً مزيفاً بنفس صوت الشخص لكنه لم يقله في الحقيقة، أو حتى عن طريق التحكم بنبرة صوت الشخص ليظهر شعور أو انطباع غير حقيقي[١].

وبالإضافة إلى ذلك، فقد أشارت الفقرة ٦٠ من المادة الثالثة من القانون إلى أن موضوع التزييف العميق قد يكون أشخاص، أو أشياء، أو أماكن، أو كيانات، أو أحداث معينة، وعلى الرغم من أن غالبية أفعال التزييف العميق كانت متعلقة بأشخاص إلا أنه يمكننا القول أن شمول التعريف لأشياء، أو أماكن، أو كيانات، أو أحداث معينة إلى جانب الأشخاص يعتبر نهجاً موسعاً محموداً لمواجهة هذه الظاهرة الجديدة وما قد يسفر عنه التقدم التكنولوجي من تزييف لمحتويات أخرى غير الأشخاص، ليشمل التزييف العميق أي شيء يمكن تحريفه أو التلاعب به من خلال تقنية التزييف العميق.

ويشير مصطلح "الكيانات" عادةً إلى المنظمات أو المؤسسات أو الهيئات الأخرى مما يعني أن القانون لا يقتصر فقط على الأشخاص، ولكنه يغطي أيضًا التحريف أو التلاعب بالكيانات مثل الشركات أو الحكومات أو المنظمات. وقد تم استخدام التزييف العميق لتزييف أحداث معينة، ومن الأمثلة الحديثة على ذلك ما حدث بالفعل في مايو ٢٠٢٣، حيث تم نشر صورة تصور انفجارًا بالقرب من (البنتاغون) عبر وسائل التواصل الاجتماعي، ومع انتشار

---

[١] دليل التزييف العميق، البرنامج الوطني للذكاء الاصطناعي، الإمارات العربية المتحدة، يوليو ٢٠٢١، ص ١٠، متاح على:

https://ai.gov.ae/ar/publications/

هذه الصورة على (تويتر) كان لها تأثير فوري على سوق الأسهم الأمريكية نتيجة تفاعل المستثمرون مع التهديد المتصور، وحاولت السلطات على الجانب الأخر نفى الخبر في محاولة لتهدئة الوضع العام في الدولة[١].

وهذا المثال يؤكد الأضرار الضخمة التي قد يمكن تحقيقها باستخدام التزييف العميق على الجوانب الاقتصادية ونشر الزعر والخوف بين عامة الناس، كما سلّط الضوء على التهديد المتزايد الذي تشكله تقنية التزييف العميق، والتي يمكن استخدامها لإنشاء محتوى إعلامي مقنع للغاية، ولكنه مُلفَق تمامًا. كما أنه من الممكن أيضًا تزييف صور لكوارث طبيعية، أو معدات عسكرية، أو أضرار الحرب، أو تدنيس للرموز، أو الشعائر الدينية بما يؤدي إلى حدوث خسائر فادحة لكل من الأمن القومي للدول والسلم الدولي على حد سواء.

ويدعم وجهة النظر هذه ظهور ما يسمى بـ "الجغرافيا المزيفة العميقة"(Deepfake geography)، والتي تشير إلى تزييف البيانات الخرائطية، بما في ذلك صور الأقمار الصناعية؛ ويمكن استخدام هذه التقنية من التزييف العميق لصنع خرائط أو نماذج تضاريس أو تصورات جغرافية مزيفة، كما يمكن من خلالها نشر خرائط معدلة تصور تغييرات الحدود لتقويض المطالبات الإقليمية، أو تعطيل الخدمات اللوجستية والتخطيط، أو حتى إثارة

---

[١] انظر في ذلك:
Luke Hurst, How a fake image of a Pentagon explosion shared on Twitter caused a real dip on Wall Street, 2023, available at: https://www.euronews.com/next/2023/05/23/fake-news-about-an-explosion-at-the-pentagon-spreads-on-verified-accounts-on-twitter [Accessed: 1 September 2024].

الصراعات الجيوسياسية. كما أن ذلك قد يؤدي إلى ضياع الثقة في مصادر البيانات الجغرافية الموثوقة[١].

ثالثاً: النتيجة الخاصة، وتتعلق هذه الخاصية بنتيجة استخدام التزييف العميق. وفي هذا الصدد، يمكننا القول إن نتيجة فعل التزييف العميق ذات طبيعة خاصة؛ ولعل ذلك يكمن في أن هذا الفعل ينتج عنه ثلاثة آثار. أما الأول فهو المحتوى المزيف، وهو نتيجة فعل التزييف العميق، في حين ينصب الأثر الثاني في النتيجة المباشرة لفعل التزييف، والذي يتمثل في خداع المتلقين نتيجة ظهور المحتوى المزيف على أنه محتوى أصلي وصحيح. أما الأثر الثالث فيتمثل في نتيجة هذا الخداع، والتي قد تكون بهدف تحقيق أرباح تجارية، أو تشويه سمعة بعض الأشخاص، أو تحقيق أغراض سياسية، أو أضرار اقتصادية، أو غير ذلك. ويجب تحقق هذه الآثار للقول بتحقق نتيجة فعل التزييف العميق.

كما يجب الإشارة في هذا الصدد، إلا أنه في استبيان تم إجراءه لتحديد أهم خصائص فعل التزييف العميق، نتج عنه اتفاق الفقهاء على خاصيتين إلزاميتين. أولهما أن يكون إنشاؤه أو التلاعب به باستخدام تقنيات الذكاء الاصطناعي (الطبيعة التقنية)، وثانيهما أن ينتج عنه إيهام الشخص بأمر على غير حقيقته، يتمثل في ظهور محتوى خاطئ في صورة محتوى صحيح وأصيل[٢].

---

[١] انظر في ذلك:

Bo Zhao et al., Deep fake geography? When geospatial data encounter Artificial Intelligence, Cartography and Geographic Information Science, vol. 48, no. 4, pp. 338–352, 2021. Available at: https://www.tandfonline.com/doi/full/10.1080/15230406.2021.1910075 [Accessed: 1 September 2024].

[٢] انظر في ذلك:

ويعتبر نص قانون الذكاء الاصطناعي على تعريف للتزييف العميق هو اتجاه جيد وحديث في تشريعات الاتحاد الأوروبي، فعلى العكس من ذلك، لم يذكر قانون الخدمات الرقمية (Digital Services Act)[١]، الصادر عن الاتحاد الأوروبي بشأن السوق الموحدة للخدمات الرقمية، أي تعريف قانوني للتزييف العميق، ولكنه أشار إلى هذه الظاهرة في المادة ٣٥(١) المتعلقة بتخفيف المخاطر (Mitigation of risks)، والتي تضمنت التزام مقدمي المنصات

Angelica Fernandez, "Deep fakes": disentangling terms in the proposed EU Artificial Intelligence Act, UFITA Archiv für Medienrecht und Medienwissenschaft, vol. 85, no. 2, pp. 392–433, 2021. Available at: https://shorturl.at/vSEdL (Accessed: 1 September 2024).

[١] قانون الخدمات الرقمية هو قانون صادر من الاتحاد الأوروبي يهدف، كجزء من "الاستراتيجية الرقمية لأوروبا" إلى إنشاء فضاء رقمي أكثر أمانًا يتم فيه حماية الحقوق الأساسية للمستخدمين وخلق تكافؤ الفرص للشركات. كما ينظم هذا القانون الوسطاء عبر الانترنت والمنصات الرقمية مثل الأسواق والشبكات الاجتماعية ومنصات مشاركة المحتوى ومنصات السفر والإقامة عبر الإنترنت. ويتمثل هدفه الرئيسي في منع الأنشطة غير القانونية والضارة عبر الإنترنت وانتشار المعلومات المضللة بما يضمن سلامة المستخدم ويحمي الحقوق الأساسية ويخلق بيئة عادلة ومنفتحة للمنصات عبر الإنترنت. وقد صدر هذا القانون بموجب التوجيه رقم ٢٠٦٥/٢٠٢٢ الصادر عن البرلمان الأوروبي والمجلس بتاريخ ٢٠٢٢/١٠/١٩ بشأن السوق الموحدة للخدمات الرقمية ودخل حيز التنفيذ في ٢٠٢٢/١١/١٦.

انظر في ذلك:

The Digital Services Act package, The European Commission, 25 July 2024, available at:

https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package [Accessed: 1 September 2024].

الإلكترونية ومحركات البحث الإلكترونية الكبيرة باتخاذ مجموعة من التدابير المعقولة والمتناسبة والفعالة لتخفيف مخاطر الاستخدامات الرقمية والتي تشمل ضمان تمييز أي عنصر من المعلومات، سواء كان صورة أو تسجيل صوتي أو فيديو، تم إنشاؤه أو التلاعب به بحيث يشبه أشخاص أو أشياء أو أماكن أو كيانات أو أحداث أخرى موجودة بالفعل، وتبدو –على غير الحقيقة– لشخص ما أنها أصلية أو صحيحة، ويكون هذا التمييز من خلال علامات بارزة عند تقديمها عبر الإنترنت، بالإضافة إلى توفير وسيلة سهلة الاستخدام تمكن متلقي الخدمة من الإشارة إلى هذه المعلومات[١].

على أن مصطلح "التزييف العميق" ذاته لم يظهر للمرة الأولى في قانون الذكاء الاصطناعي في تشريعات الاتحاد الأوروبي، فقد تم ذكره بالفعل في بعض التوجيهات واللوائح التي صدرت من البرلمان الأوروبي والمجلس الأوروبي، والتي نذكر منها على سبيل المثال المقترح المتعلق بالتوجيه الأوروبي

---

[١] المادة ٣٥ من قانون الخدمات الرقمية السابق الإشارة إليه، والتي تنص على:
"1. Providers of very large online platforms and of very large online search engines shall put in place reasonable, proportionate and effective mitigation measures, tailored to the specific systemic risks identified pursuant to Article 34, with particular consideration to the impacts of such measures on fundamental rights. Such measures may include, where applicable: ……. (k) ensuring that an item of information, whether it constitutes a generated or manipulated image, audio or video that appreciably resembles existing persons, objects, places or other entities or events and falsely appears to a person to be authentic or truthful is distinguishable through prominent markings when presented on their online interfaces, and, in addition, providing an easy to use functionality which enables recipients of the service to indicate such information".

بشأن مكافحة العنف ضد المرأة والعنف الأسري الذي أشار إلى أن الأفعال التي تشكل جرائم بموجب هذا التوجيه يجب أن تشمل "التزييف العميق".[١]

ونستنتج مما سبق أن فعل التزييف العميق هو أحد تقنيات الذكاء الاصطناعي، والذي يقع –وفقاً لقانون الذكاء الاصطناعي– على الصور والمقاطع الصوتية والفيديو، ليظهر هذا المحتوى المزيف على أنه أصلى وصحيح على خلاف الحقيقة. كما تبني القانون اتجاهًا موسعًا فيما يتعلق بإمكانية وقوع فعل التزييف العميق على أشخاص، أو أشياء، أو أماكن، أو كيانات، أو أحداث معينة، بما يضمن حماية قانونية أوسع من أضرار هذا الفعل. وسوف نتناول في المبحث التالي التنظيم القانوني لهذه التقنية على النحو الذي أورده القانون.

---

[١] انظر في ذلك:

Proposal for a Directive on combating violence against women and domestic violence, COM/2022/105 final, 2022, para. 19.

It was provided that "……. The offence should also include the nonconsensual production, manipulation or altering, for instance by image editing, including by means of artificial intelligence, of material that makes it appear as though a person is engaged in sexual activities, in so far as the material is subsequently made accessible to the public by means of ICT without the consent of that person. Such production, manipulation or altering should include the fabrication of 'deepfakes', where the material appreciably resembles an existing person, objects, places or other entities or events, depicts the sexual activities of a person, and would falsely appear to other persons to be authentic or truthful. In the interest of effectively protecting victims from such conduct, threatening to engage in such conduct should also be covered. Available at: https://rb.gy/y7rqwe [Accessed: 3 September 2024].

المبحث الثاني

التنظيم القانوني للتزييف العميق في قانون الذكاء الاصطناعي

وضحت المادة الأولى من قانون الذكاء الاصطناعي الغرض من هذا القانون، فنصت على أن "الغرض من هذه اللائحة هو تحسين أداء السوق الداخلية وتعزيز استخدام الذكاء الاصطناعي الجدير بالثقة والذي يتمحور حول الإنسان، مع ضمان مستوى عالٍ من حماية الصحة والسلامة والحقوق الأساسية المنصوص عليها في الميثاق، والتي تتضمن الديمقراطية وسيادة القانون وحماية البيئة ضد الآثار الضارة لأنظمة الذكاء الاصطناعي في الاتحاد ودعم الابتكار"[١].

كما حدّد القانون شموله لقواعد متناسقة لطرح أنظمة الذكاء الاصطناعي في السوق ووضعها في الخدمة واستخدامها في دول الاتحاد الأوروبي، كما حظر بعض ممارسات الذكاء الاصطناعي، وتضمن متطلبات محددة لأنظمة الذكاء الاصطناعي عالية المخاطر والتزامات على مقدمي ومستخدمي هذه الأنظمة، هذا بالإضافة إلى النص على بعض القواعد الخاصة بالشفافية ومراقبة السوق، وتحديد تدابير لدعم الابتكار، مع التركيز على الشركات الصغيرة والمتوسطة الحجم، بما في ذلك الشركات الناشئة[٢].

وقد تضمن مقترح قانون الذكاء الاصطناعي نهجاً خاصاً في التنظيم القانوني لأنظمة الذكاء الاصطناعي، فتضمّن ما يمكن تقسيمه إلى أربع فئات، أما الفئة الأولى فهي أفعال محظورة (Prohibited AI practices) نصت

[١] المادة ١ من قانون الذكاء الاصطناعي الصادر من الاتحاد الأوروبي.

[٢] المادة ٢ من قانون الذكاء الاصطناعي الصادر من الاتحاد الأوروبي.

عليها المادة الخامسة على سبيل الحصر، ثم تأتي الفئة الثانية لتشمل أنظمة الذكاء الاصطناعي عالية المخاطر (HIGH-RISK AI SYSTEMS) والتي تناولها الفصل الثالث من القانون، أما الفئة الثالثة فتتناول التزامات خاصة ببعض الأنشطة المحددة الأقل خطورة نظراً لأن مخاطرها محدودة(limited risk)، أما الفئة الرابعة فهي تشمل الأفعال ذات أقل قدر من المخاطر (minimal risk)[١].

وهذا التصنيف وجّه له البعض العديد من الانتقادات التي ترجع إلى أنه تصنيف "وهمي وتعسفي" نظراً لأنه لا ينطبق على "دورة حياة الذكاء

[١] على الرغم من أن "ممارسات الذكاء الاصطناعي المحظورة" و"أنظمة الذكاء الاصطناعي عالية المخاطر" فقط هي المذكورة صراحةً في القانون، إلا أن المفوضية قدمت أربع فئات من المخاطر في "الأسئلة والأجوبة حول القواعد الجديدة للذكاء الاصطناعي"، انظر في ذلك:
European Commission, 'New Rules for Artificial Intelligence – Questions and Answers,' Text, 2021, available at: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683

الاصطناعي"[١] بالكامل، كما أنه يستبعد أو لا يغطي بالكامل بعض أشكال الاستخدامات الضارة لبعض أنظمة الذكاء الاصطناعي[٢].

وعلى كل حال، فإن القانون في تنظيمه للقواعد القانونية الخاصة بأنظمة الذكاء الاصطناعي قد تناول هذه الأنظمة في ثلاث فئات. حيث حظر بعض الأنظمة في المادة الخامسة من القانون، وأورد قواعد خاصة للأنظمة عالية المخاطر في الفصل الثالث من القانون بدءًا من المادة السادسة، ثم أورد قواعد خاصة لأنظمة محددة في الفصل الرابع من القانون.

ولتحديد القواعد القانونية التي تطبق على التزييف العميق، يجب أولاً تحديد الفئة التي يقع ضمنها على النحو الذي أورده القانون، وهو أمر ليس بالسهل لأنه يعتمد على مجموعة من المعايير والعوامل. وتعتمد هذه المعايير والعوامل بدورهاعلى تحديد الاستخدامات المحتملة لهذه التقنية، والتي قد تختلف بالتأكيد من حالة إلى أخرى. وبذلك، لا ينبغي النظر فقط إلى الجانب الضار

---

[١] تعرف دورة حياة نظام الذكاء الاصطناعي بأنها "هي المنهجية التي يتم اتباعها عند تنفيذ مشاريع الحلول التقنية المعتمدة على تقنيات الذكاء الاصطناعي، والتي بموجبها يتم تحديد كل خطوة يتوقع من الجهة اتباعها للاستفادة من هذه التقنية لتحقيق قيمة عملية، وهي طريقة موحدة لتمثيل المهام استناداً إلى أفضل الممارسات في تنفيذ وإدارة نماذج الذكاء الاصطناعي، مما يجعلها أنسب الخيارات لتضمين أخلاقيات الذكاء الاصطناعي". وتشمل هذه الدورة أربع مراحل هي التخطيط والتصميم، وتهيئة البيانات، البناء وقياس الأداء، التطبيق والمتابعة، انظر في ذلك:

تقرير الهيئة السعودية للبيانات والذكاء الاصطناعي، مبادئ أخلاقيات الذكاء الاصطناعي، أغسطس ٢٠٢٢، ص ٥، متاح على: https://shorturl.at/jv5fA

[٢] انظر في ذلك:

Lilian Edwards, Regulating AI in Europe: four problems and four solutions, Ada Lovelace Institute, 2022, p. 5, available at: https://shorturl.at/qCgfY [Accessed: 14 August 2024],

للتزييف العميق، الذي قد يمثل شكلاً خطيرًا من أشكال التلاعب الصوتي والبصري، حيث توجد العديد من التطبيقات الإيجابية لهذه التقنية. فلا ينبغي وصف هذه التقنية بأنها ضارة بطبيعتها، بل يجب اعتبارها "محايدة"[١].

وعلى ذلك، فإن استخدامات التزييف العميق هي التي تمنحها بعدًا معينًا، والأهداف وراء إنشائها أو نشرها هي التي تضعها في سياق محدد. وعلى الرغم من أن التعريف الذي قدمناه لم يشمل 'سياق الاستخدام' من بين العناصر اللازمة للتعريف، إلا أنه لا يمكن تجاهله، باعتباره قد يشكل عاملاً رئيسيًا في تقييم خطورة الفعل. فنجد أن التركيز على الاستخدامات السلبية للتزييف العميق أدى إلى منحه سمعة سيئة، مع إنكار كل أثر إيجابي لهذه التقنية، مما قد يؤدي إلى تقييم غير مناسب للخطورة الناتجة عن استخدامه، ويقوض التقدم العلمي والتكنولوجي الذي تحقق بفضل استخدامه. ويمكن التوصل إلى هذه النتيجة أيضًا بالنظر إلى المصطلح المستخدم لهذه التقنية، وهو 'التزييف العميق'، دون النظر إلى الاستخدامات الإيجابية لهذه التقنية.

وبدايةً يمكن القول إن قانون الذكاء الاصطناعي لم يحظر تقنية التزييف العميق بشكل تام، ولعل ذلك يكمن في إدراكه لوجود جانب إيجابي لهذه التقنية. فبداية ظهورها في بعض الاستخدامات السلبية هو ما ساهم في ترسيخ الفكرة

---

[١] انظر في ذلك:

Adrienne de Ruiter, The Distinct Wrong of Deepfakes, Philosophy & Technology, vol. 34, pp. 1311–1332, 2021, p. 1313, available at: https://link.springer.com/article/10.1007/s13347-021-00459-2 [Accessed: 14 August 2024].

السلبية عن هذه التقنية في أذهان البعض[١]. وهذا الرأي له ما يبرره، فكما أشار خبراء وكالة الاتحاد الأوروبي للتعاون في مجال إنفاذ القانون (EUROPOL) فإن معظم المحتويات التي تتم باستخدام التزييف العميق تكون بقصد الإضرار[٢].

وبالإضافة إلى ذلك، فإن السمة الجوهرية للتزييف العميق هي أنه يزيد من اللبس من خلال طمس الحدود بين العمل الأصلي والعمل غير الأصلي، ويجعل من الصعب التمييز بين الحقيقة والخيال مما يعزز بشكل كبير من إمكانية التضليل الرقمي[٣]. وبالتالي، يجب عند تقييم المخاطر المحتملة للتزييف

---

[١] حيث يشير البعض إلى أن بداية ظهور هذه التقنية كانت من خلال الاستخدام في أعمال إباحية ولعل ذلك السبب وراء هذا الاعتقاد من أن هذه التقنية ذات أثر سلبي فقط، انظر في ذلك:

Casey Becker and Robin Laycock , Embracing deepfakes and AI-generated images in neuroscience research, European Journal of Neuroscience, vol. 58, no. 3, pp. 2657–2661, 2023, p. 2657, available at: https://onlinelibrary.wiley.com/doi/10.1111/ejn.16052 [Accessed: 14 August 2024].

انظر أيضاً:

Bart van der Sloot et al, Deepfakes: The Legal Challenges of the Synthetic Society, Tilburg Institute for Law, Technology, and Society, 2021, p. 2, available at: https://shorturl.at/Hz38W [Accessed: 15 August 2024].

[٢] انظر في ذلك:

Europol, Facing reality? Law enforcement and the challenge of deepfakes, an observatory report from the Europol Innovation Lab, Publications Office of the European Union, 2022, pp. 19-20, available at: https://shorturl.at/fBe72 [Accessed: 15 August 2024].

[٣] انظر في ذلك:

Cristian Vaccari and Andrew Chadwick, Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News, Social Media + Society, vol. 6, no. 1, 2020, p. 2, available at: https://journals.sagepub.com/doi/10.1177/2056305120903408 [Accessed: 15 August 2024].

العميق، أن يُؤخَذ في الاعتبار النتائج السلبية الذي يسببها داخل فضاء المعلومات، بما في ذلك تقويض الثقة في المعلومات أو وسائل الإعلام.

وتجدر الإشارة إلى أن القانون، بطبيعة الحال، يطبق على مقدمي الخدمة والمستخدمين المقيمين أو الذين يقع مقر تأسيسهم داخل دول الاتحاد الأوروبي، أو في الحالة التي تُنتج فيها مخرجات نظام الذكاء الاصطناعي في الاتحاد، أو في حالة حدوث ضرر لأشخاص موجودين داخل الاتحاد، حتى لو كان مكان الإقامة أو مقر التأسيس خارج الاتحاد، باستثناء الأنظمة المستخدمة لأغراض عسكرية أو دفاعية أو أمنية[١].

كما استثنت المادة الثانية من القانون الأنظمة المستخدمة من السلطات العامة في دولة أخرى أو المنظمات الدولية طبقًا لهذا القانون، وذلك عندما يكون استخدامها في إطار التعاون الدولي أو اتفاقيات إنفاذ القانون والتعاون القضائي مع الاتحاد أو مع دولة أو أكثر من الدول الأعضاء، شريطة أن توفر هذه الدولة الأخرى أو المنظمة الدولية ضمانات كافية فيما يتعلق بحماية الحقوق والحريات الأساسية للأفراد[٢].

وعلى الرغم من أن القانون لم يتعرض للمسؤولية الدولية في هذا السياق، إلا أن ذلك لا يمنع من إمكانية تطبيقها متى توافرت الشروط القانونية لذلك وفقًا للقواعد العامة للمسؤولية الدولية. فنص القانون عند تعريف مقدم الخدمة والمستخدم بأنه 'شخص طبيعي، أو اعتباري، أو سلطة عامة، أو وكالة، أو هيئة أخرى...' يمكن أن يُستفاد منه أنه قد تثار المسؤولية الدولية عند استخدام السلطة

---

[١] المادة ٢ من قانون الذكاء الاصطناعي الصادر من الاتحاد الأوروبي.

[٢] انظر في ذلك:

Ibid.

العامة للدولة لأنظمة الذكاء الاصطناعي، أو الأشخاص الطبيعيين أو الاعتباريين متى تم إسناد هذا الفعل إلى الدولة وفقًا لقواعد الإسناد[١].

وفي كل الأحوال، في حين أن الدول تتمتع بحرية في استخدام ما لديها من إمكانات في مجال الذكاء الاصطناعي بما يحقق مصالحها الوطنية والدولية، إلا أن هذه الحرية ليست مطلقة، فهي مقيدة بمبدأ حسن النية في التعاملات الدولية وعدم الإضرار بالغير، وإلا ستكون عرضة لتوقيع العقوبات عليها[٢].

ونظراً للنهج الذي تبناه القانون في التنظيم القانوني لأنظمة الذكاء الاصطناعي القائم على الخطورة (Risk-based Approach)، والتقسيم المتبع إلى فئات معينة ينطبق على كل منها قواعد محددة، بما في ذلك الممارسات المحظورة، والأنظمة عالية المخاطر، وأنظمة معينة ينطبق عليها

---

[١] تعرف المسؤولية الدولية بأنها "مجموعة القواعد القانونية التي تحكم أي عمل أو واقعة تنسب إلى أحد أشخاص القانون الدولي وينجم عنها ضرر لشخص اخر من أشخاص القانون الدولي وما يترتب على ذلك من التزام بالتعويض". انظر في ذلك:

أ.د/ صلاح الدين عامر، مقدمة لدراسة القانون الدولي العام، طبعة ٢٠٠٢، دار النهضة العربية، ص ٧٢٦.

وتعرف أيضًا بأنها "وضع قانوني، تلتزم بمقتضاه الدولة المنسوب إليها القيام بعمل أو نشاط ما بتعويض الضرر الذي يصيب دولة أخرى أو أحد رعاياها نتيجة هذا العمل أو النشاط". انظر في ذلك:

أ.د/ محمد طلعت الغنيمي، الوسيط في القانون الدولي العام، الدار الجامعية، طبعة ٢٠٠٣، ص ٢٦٠.

وللمزيد عن المسؤولية الدولية، انظر في ذلك:

أ.د/ أحمد أبو الوفا، الوسيط في القانون الدولي العام، دار النهضة العربية، طبعة ٢٠٠٤، ص ٣٢٢.

[٢] د/ أبو الخير عطيه، قانون التنظيم الدولي، مطبعة الفجيرة الوطنية، دبي، طبعة ٢٠٠٧، ص ٢٧٠.

التزامات محددة، فإنه يجب تحليل الفئة التي يقع ضمنها فعل التزييف العميق. وعلى ذلك سوف نقوم بتقسيم هذا المبحث إلى عدة مطالب على النحو التالي:

المطلب الأول: مدى إمكانية اعتبار التزييف العميق ضمن الممارسات المحظورة

المطلب الثاني: مدى إمكانية اعتبار التزييف العميق ضمن الفئات عالية الخطورة

المطلب الثالث: تطبيق الالتزام بالشفافية والتمييز على التزييف العميق

المطلب الأول

مدى إمكانية اعتبار التزييف العميق ضمن الممارسات المحظورة

عند النظر إلى قانون الذكاء الاصطناعي، نجد أنه اعتبر بعض الأفعال ذات خطورة كبيرة، فقرر حظرها بالنص عليها صراحةً في المادة الخامسة من القانون. وقد ركّزت هذه الفئة الأولى على الأفعال التي تتعارض مع قيم الاتحاد الأوروبي وتشكل انتهاكاً للحقوق الأساسية. وهذه الممارسات محددة على سبيل الحصر، ويمكن تلخيصها في حظر الطرح في السوق أو تشغيل أو استخدام أنظمة الذكاء الاصطناعي الآتية[١]:

- أنظمة الذكاء الاصطناعي ذات طبيعة خفية خارجة عن وعي الشخص أو ذات طبيعة تحايلية أو مخادعة بشكل متعمد، مع خطر التسبب في ضرر كبير؛
- أنظمة الذكاء الاصطناعي التي تستغل نقاط ضعف الأشخاص بطريقة يمكن أن تسبب ضررًا كبيرًا؛

[١] المادة ٥ من قانون الذكاء الاصطناعي الصادر من الاتحاد الأوروبي.

– أنظمة الذكاء الاصطناعي المستخدمة لتصنيف أو تسجيل الأشخاص بناءً على السلوك أو الخصائص الشخصية مما يؤدي إلى معاملة ضارة؛

– التنبؤ البوليسي (Predictive policing) القائم على التصنيف باستخدام الذكاء الاصطناعي أو تقييم الذكاء الاصطناعي للسمات الشخصية؛

– الكشط غير المقصود لصور الوجه لإنشاء قواعد بيانات للتعرف على الوجه باستخدام الذكاء الاصطناعي؛

– أنظمة الذكاء الاصطناعي المستخدمة للتعرف على العواطف في أماكن العمل والتعليم؛

– التصنيف الحيوي (البيومتري)[١] (Biometric categorization) لأنظمة الذكاء الاصطناعي لاستنتاج السمات الشخصية الحساسة؛

– أنظمة الذكاء الاصطناعي المستخدمة في التعرف البيومتري عن بعد في وقت محدد في الأماكن التي يمكن الوصول إليها للعامة لأغراض إنفاذ القانون.

وأول ما يلاحظ على هذه الممارسات أنها لم تتضمن حظر تقنية التزييف العميق صراحةً. ولعل ذلك نتيجة إدراك المشرع للجانب الإيجابي لهذه التقنية، فكما أنه يُستخدَم لتحقيق أضرار معينة، فإنه يمكن استخدامه أيضا لأغراض

[١] يشير التصنيف الحيوي (البيومتري) إلى تصنيف الأفراد أو المجموعات على أساس البيانات المتعلقة بأجسادهم وسلوكياتهم إلى فئات محددة – مثل الجنس، أو العمر، أو السمات السلوكية، أو الشخصية، أو التوجه الجنسي، أو التوجه السياسي – بناءً على بياناتهم الحيوية (البيومترية). انظر في ذلك:
David J. Oberly, Analyzing the EU Artificial Intelligence Act: Spotlight on Biometrics, Baker Doneslon, 16 May 2024, available at: https://shorturl.at/N3n6k [Accessed: 18 August 2024]

إيجابية. وبذلك، لم يكن من الحكمة حظر هذه التقنية بشكل مطلق، بل تنظيمها بصورة أفضل.

ولكن هل يعني عدم النص الصريح على فعل التزييف العميق في المادة الخامسة من القانون أنه لا يمكن أن يكون محظوراً بأي حال من الأحوال بموجب هذه المادة؟

الحقيقة أن التطرق لنص الفقرة الأولى من المادة الخامسة قد يؤدي إلى نتيجة مختلفة، فقد نصت على أن حظر: (أ) الطرح في السوق أو تشغيل أو استخدام تقنيات ذكاء اصطناعي ذات طبيعة خفية خارجة عن وعي الشخص أو ذات طبيعة تحايلية أومخادعة بشكل متعمد، لهدف أو للتأثير في تشويه سلوك شخص أو مجموعة من الأشخاص بشكل مادي من خلال إضعاف قدرتهم على اتخاذ قرار مستنير بشكل ملحوظ، مما يدفعهم إلى اتخاذ قرار لم يكونوا ليتخذوه لولا ذلك بطريقة تُسبِب أو من المُحتمَل أن تسبب ضررًا كبيرًا لذلك الشخص أو شخص آخر أو مجموعة من الأشخاص"[١].

وبالنظر إلى المصطلح الوارد في الفقرة السابق "تقنيات تحايلية أو مخادعة" (manipulative or deceptive techniques) نجد أن القانون لم

---

[١] انظر في ذلك: المادة ٥/١/أ من قانون الذكاء الاصطناعي والتي تنص على:
"1. The following AI practices shall be prohibited: (a) the placing on the market, the putting into service or the use of an AI system that deploys subliminal techniques beyond a person's consciousness or purposefully manipulative or deceptive techniques, with the objective, or the effect of materially distorting the behaviour of a person or a group of persons by appreciably impairing their ability to make an informed decision, thereby causing them to take a decision that they would not have otherwise taken in a manner that causes or is reasonably likely to cause that person, another person or group of persons significant harm".

يحدد المقصود بها، كما لم يُعدِد التقنيات التي يمكن اعتبارها من قبيل ذلك، واكتفي بذكر الغرض من هذه التقنيات. وعند محاولة تفسير النص نجد أنه كقاعدة عامة عند تفسير تشريعات الاتحاد الأوروبي، فإن نقطة البداية، كما هو الحال مع القانون المحلي، هو النظر إلى الألفاظ المستخدمة. فإذا كان التشريع غامضًا، يتم استخدام طرق التفسير التي تحدد الغرض منه وذلك من خلال النظر في ديباجة القانون (recitals) أو الأعمال التحضيرية[١].

وقد أشارت محكمة العدل الأوروبية (ECJ) إلى هذا المعنى، فأكدت أنه متى كان النص غامضاً، فإنه يمكن تفسيره وفقاً للغرض منه[٢]. وعند البحث حول معني "تقنيات تحايلية أو مخادعة" نجد أن كلمة (مخادعة) (deceptive) تعني "جعل الشخص يصدق ما هو غير صحيح، فهو يظهر على غير حقيقته"[٣].

---

[١] انظر في ذلك:

Ziolkowski and others v Land Berlin, Case C-424/10 and C-425/10, EU:C:2011:866, 2011, paragraphs 37, 42 and 43, available at: https://eu.vlex.com/vid/judgment-of-the-court-838702989

The Court relied on recitals to ascertain the purpose of the Citizenship Directive, and the structured nature of the rights contained in it.

[٢] انظر في ذلك:

Case C-803/79 Gérard Roudolff EU:C:1980:166, para 7, available at: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A61979CJ0803

The Court declared that where the text is ambiguous, it shall be examined in light of its purpose.

[٣] انظر في ذلك:

The meaning of deceptive, The Cambridge dictionary, available at: https://dictionary.cambridge.org/dictionary/english/deceptive

Deceptive means " making you believe something that is not true".

وبالرجوع إلى التزييف العميق والتعريف الذي أورده القانون في الفقرة ٦٠ من المادة الثالثة بأنه "صورة أو محتوى صوتي أو فيديو تم إنشاؤه أو التلاعب به بواسطة الذكاء الاصطناعي بهدف مماثلة أشخاص، أو أشياء، أو أماكن، أو كيانات، أو أحداث معينة، ويظهر –على غير الحقيقة– للشخص العادي أنه أصلي أو صحيح"، نجد أنه يكون له نتيجة مباشرة تتمثل في الخداع أو التلاعب بإدراك الأشخاص بظهور المحتوى على عكس حقيقته. وبالتالي، فالخداع يشكل جوهر فعل التزييف العميق.

وعلى ذلك فإنه يمكننا من خلال مقاربة هذه النصوص التوصل إلى أنه يمكن اعتبار التزييف العميق فعلاً محظوراً طبقاً للفقرة الأولى من المادة الخامسة متى توافرت شروط معينة هي:

الشرط الأول: الطرح في السوق[١] أو تشغيل أو استخدام نظام ذكاء اصطناعي ذي طبيعة مخادعة مُتعمَدة تتجاوز وعي الشخص. ولما كان التزييف العميق هو أحد أنظمة الذكاء الاصطناعي، فيتوافر هذا الشرط بمجرد الطرح في السوق أو التشغيل أو الاستخدام للتزييف العميق بشرط أن يكون الخداع متعمداً؛

[١] حددت المادة الثالثة من القانون المقصود بـ "الطرح في السوق" بأنه الطرح الأول لجعل نظام الذكاء الاصطناعي أو نموذج الذكاء الاصطناعي متاحاً للأغراض العامة في سوق الاتحاد. ويكون متاحاً في السوق بتوفير نظام الذكاء الاصطناعي أو نموذج الذكاء الاصطناعي للأغراض العامة للتوزيع أو الاستخدام في السوق في سياق نشاط تجاري، سواء بمقابل أو بدون مقابل. انظر في ذلك:
الفقرتان ٩ و١٠ من المادة ٣ من قانون الذكاء الاصطناعي الصادر من الاتحاد الأوروبي.

الشرط الثاني: أن يكون استخدام التزييف العميق بهدف التأثير في تشويه سلوك شخص أو مجموعة من الأشخاص بشكل ملموس، وأن يؤدي ذلك إلى إضعاف قدرتهم على اتخاذ قرار مستنير بشكل ملحوظ، مما يدفعهم إلى اتخاذ قرار لم يكونوا ليتخذوه لولا ذلك؛

الشرط الثالث: أن يؤدي ذلك إلى التسبب أو من المحتمل أن يتسبب في ضرر كبير لذلك الشخص أو غيره أو مجموعة من الأشخاص.

ونتيجةً لذلك فإن فعل التزييف العميق يعتبر فعلاً محظوراً بموجب المادة الخامسة من قانون الذكاء الاصطناعي متى نتج عنه تأثير في سلوك شخص أو أشخاص أو إضعاف قدرتهم على اتخاذ قرار للدرجة التي تغير من القرار ذاته بحيث ما كان ليتخذه لولا ذلك التأثير، وترتّب على ذلك حدوث ضرر أو احتمالية حدوث ضرر.

وقد نصت المادة ٣/٩٩ من القانون على عقوبة عدم الامتثال لهذا الحظر فنصت على أنه "يُعاقَب على عدم الامتثال لحظر ممارسات الذكاء الاصطناعي المنصوص عليها في المادة ٥ بغرامات إدارية تصل إلى ٣٥ مليون يورو أو، إذا كان الجاني مؤسسة، ما يصل إلى ٧٪ من إجمالي مبيعاتها السنوية العالمية للسنة المالية السابقة، أيهما أعلى"[١].

وهنا يثور التساؤل عن الوضع في حالة فقدان فعل التزييف العميق لهذه الشروط أو أحداهما، أو بمعنى آخر ما هو التنظيم القانوني للتزييف العميق إذا

[١] المادة ٣/٩٩ من قانون الذكاء الاصطناعي الصادر من الاتحاد الأوروبي.

لم يصل إلى حد الفعل المحظور وفقاً للمادة الخامسة من القانون؟ وهو ما سنحاول الإجابة عنها في المطلب التالي.

المطلب الثاني

مدى إمكانية اعتبار التزييف العميق ضمن الفئات عالية الخطورة

تضمّن قانون الذكاء الاصطناعي فئة ثانية من أنظمة الذكاء الاصطناعي والتي تشمل الأنظمة عالية الخطورة (HIGH-RISK AI SYSTEMS)، وهي الأفعال التي قد تخلق تأثيرًا سلبيًا بدرجة عالية من الخطورة على سلامة الأشخاص أو حقوقهم الأساسية التي يحميها ميثاق الحقوق الأساسية للاتحاد الأوروبي[١]، وقد حددت المادة ٦ من قانون الذكاء الاصطناعي المتطلبات اللازمة لتصنيف أنظمة الذكاء الاصطناعي على أنها عالية الخطورة بهدف ضمان الرقابة الصارمة لحماية السلامة العامة والحقوق الأساسية، وقسّمت هذه الأنظمة إلى فئتين، وتشمل الفئة الأولى أنظمة توصف بأنها عالية الخطورة بتوافر شرطين أساسيين هما:

الشرط الأول: أنظمة الذكاء الاصطناعي التي تكون هي بحد ذاتها منتج، أو أحد عناصر الأمان[٢] في منتج طبقاً لتشريعات الاتحاد الواردة في الملحق الأول للقانون؛

---

[١] الفقرة ٤٨ من ديباجة قانون الذكاء الاصطناعي الصادر من الاتحاد الأوروبي.

[٢] يقصد بـ"أحد عناصر الأمان" أن يكون نظام الذكاء الاصطناعي يقوم بوظيفة الأمان كمنتج أو عنصر أمان في نظام ذكاء اصطناعي، بحيث يؤدي فشله أو خلله إلى تعريض صحة وسلامة الأشخاص أو الممتلكات للخطر. انظر في ذلك:
الفقرة ١٤ من المادة ٣ من قانون الذكاء الاصطناعي للاتحاد الأوروبي.

الشرط الثاني: أنظمة الذكاء الاصطناعي التي تتطلب استيفاء "متطلب تقييم المطابقة"[١] (Third-Party Conformity Assessment) من قبل الغير (طرف ثالث) طبقاً لتشريعات الاتحاد الواردة في الملحق الأول للقانون لضمان استيفائها لمعايير السلامة والأخلاق الصارمة قبل طرحها في السوق[٢].

فكما أشارت ديباجة القانون إلى أنه قد يكون لأنظمة الذكاء الاصطناعي تأثير سلبي على صحة وسلامة الأشخاص، وخاصةً عندما تعمل هذه الأنظمة كمكونات أمان للمنتجات. وتماشياً مع أهداف تشريعات الاتحاد لتسهيل حرية حركة المنتجات في السوق الداخلية وضمان وصول المنتجات الآمنة والمتوافقة فقط إلى السوق، من المهم منع المخاطر المتعلقة بالسلامة التي قد تولدها المنتجات بسبب مكوناتها الرقمية، بما في ذلك أنظمة الذكاء الاصطناعي، وتخفيف أضرارها. فعلى سبيل المثال، يجب أن تكون الروبوتات، سواء المُستخدَمة في التصنيع أو المساعدة أو الرعاية الشخصية، قادرة على العمل بأمان وأداء وظائفها في ظروف معقدة. وبالمثل، في قطاع الصحة حيث تكون المخاطر على الحياة والصحة عالية، يجب أن تكون أنظمة التشخيص وأنظمة

---

[١] تقييم المطابقة هو العملية التي يقوم بها المصنع لإثبات ما إذا كانت المتطلبات المحددة المتعلقة بالمنتج قد تم الوفاء بها، ويخضع المنتج لتقييم المطابقة أثناء مرحلة التصميم والإنتاج. وذلك بغرض التأكد من أن هذا المنتج يلبي جميع المتطلبات التشريعية الخاصة بالمنتج، ويشمل ذلك التقييم عدة مراحل هي الاختبار والتفتيش والشهادة، وتحدد تشريعات المنتج المعمول بها الإجراء الخاص بكل منتج. انظر في ذلك:
INFORMATION FROM EUROPEAN UNION INSTITUTIONS, BODIES, OFFICES AND AGENCIES, EUROPEAN COMMISSION, COMMISSION NOTICE The 'Blue Guide' on the implementation of EU product rules 2022, (2022/C 247/01), 29 June 2022, para. 5, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022XC0629(04)

[٢] الفقرة ٦ من قانون الذكاء الاصطناعي الصادر من الاتحاد الأوروبي.

الدعم موثوقة ودقيقة[١]. وحيث أن التزييف العميق لا يمكن أن يكون منتج أو أحد عناصر الأمان في منتج كما أنه لم يتم النص عليه في تشريعات الاتحاد المشار إليها، فبالتالي لا يمكن اعتباره ضمن الأنظمة عالية الخطورة في هذه الفئة.

أما الفئة الثانية من الأنظمة عالية الخطورة فقد تضمنتها الفقرة الثانية من المادة السادسة من القانون بنصها على أنه "تعتبر أنظمة الذكاء الاصطناعي المشار إليها في الملحق الثالث أنظمة عالية الخطورة"[٢]، وقد تضمن الملحق الثالث (ANNEX III) قائمة لبعض القطاعات التي اعتبر القانون أن أنظمة الذكاء الاصطناعي المستخدمة فيها تعتبر عالية الخطورة، مع قابلية هذه القائمة للمراجعة لتتوافق مع تطور استخدامات أنظمة الذكاء الاصطناعي. وتشمل هذه الفئة مجموعة من المجالات التي قسّمها المشرع وفقاً لنظام قطاعي (Sectorial) واعتبر أنظمة الذكاء الاصطناعي المستخدمة فيها عالية الخطورة نظراً لطبيعتها الخاصة وأهميتها في الحفاظ على الحقوق والحريات الأساسية[٣].

وبذلك يمكننا القول، أن المشرع قد قدّر أن أنظمة الذكاء الاصطناعي المُستخدَمة في هذه القطاعات تُعتبَر عالية الخطورة نظراً لأهميتها وبسبب تأثيرها المحتمل على السلامة العامة والحقوق الأساسية، فكما أشارت ديباجة القانون أن أنظمة الذكاء الاصطناعي قد ينتج عنها تأثيراً سلبياً على الحقوق الأساسية

---

[١] الفقرة ٤٧ من ديباجة قانون الذكاء الاصطناعي الصادر من الاتحاد الأوروبي.

[٢] المادة ٢/٦ من قانون الذكاء الاصطناعي الصادر من الاتحاد الأوروبي.

[٣] انظر في ذلك:

Annex III High-risk AI systems referred to in Article 6(2), REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL No. 2024/1689, 13 June 2024.

التي يحميها ميثاق الحقوق الأساسية وهو ما يكون له أهمية خاصة عند تصنيف هذه الأنظمة واعتبارها عالية الخطورة. وتشمل هذه الحقوق الحق في الكرامة، والحق في احترام الحياة الخاصة والعائلية، وحماية البيانات الشخصية، وحرية التعبير والمعلومات، وحرية التجمع وتكوين الجمعيات، والحق في عدم التمييز، والحق في التعليم، وحماية المستهلك، وحقوق العمال، وحقوق الأشخاص ذوي الإعاقة، والمساواة بين الجنسين، وحقوق الملكية الفكرية، والحق في الانتصاف الفعال والمحاكمة العادلة، والحق في الدفاع وافتراض البراءة، والحق في الإدارة الجيدة[١].

وكما ذكرنا، فقد استخدم المشروع في هذه الفئة تقسيم قطاعي أي أنه اعتبر الأنظمة المتعلقة بهذه القطاعات الواردة في الملحق الثالث للقانون هي أنشطة عالية الخطورة، وبذلك لم يعدد الأفعال ذاتها كما هو الحال بالنسبة للفئة الأولى الخاصة بالممارسات المحظورة الواردة في المادة الخامسة. **وهنا يثور التساؤل عما إذا كان من الممكن اعتبار التزييف العميق من قبل الأنظمة عالية الخطورة إذا تم استخدامه في سياق أحد القطاعات الواردة بالملحق الثالث؟**

للإجابة على هذا التساؤل، يجب الإشارة إلى أنه قد يبدو للوهلة الأولى أن عدم ذكر التزييف العميق صراحة في الفئة الثانية (عالية الخطورة)، قد يؤدي إلى نتيجة حتمية مفادها أن قانون الذكاء الاصطناعي قد اعتبر التزييف العميق من قبيل أنظمة الذكاء الاصطناعي محدودة أو منخفضة الخطورة المشمولة

[١] الفقرة ٤٨ من ديباجة قانون الذكاء الاصطناعي الاتحاد الأوروبي.

بالتزامات الشفافية فقط المنصوص عليها في الفصل الخامس من القانون، والتي سنتناولها في المطلب التالي بالتفصيل[١].

إلا أن هذا الاستنتاج قد يكون غير صحيح –من وجهة نظر الباحث– لعدة أسباب:

أولاً: أن القانون قد قسم أنظمة الذكاء الاصطناعي إلى ممارسات محظورة في المادة الخامسة، وأنظمة عالية المخاطر في المادة السادسة. وفي المادة الخامسة عدّد الأفعال المحظورة نفسها والتي سبق شرحها في المطلب السابق، أما بالنسبة للأنظمة عالية الخطورة فقد اتبع المشرع نهجاً قائماً على التقسيم إلى قطاعات أوردها في الملحق الثالث وليس ممارسات معينة كما هو الحال في المادة الخامسة من القانون. وبالتالي فإن عدم النص الصريح على فعل التزييف العميق في الملحق الثالث لا يعنى أنه لا يمكن اعتباره من الأنظمة عالية الخطورة.

ثانياً: أن عنوان الفصل الخامس نفسه –الذي نص صراحة على فعل التزييف العميق– هو "التزامات الشفافية لمُقدِمي ومُستخدِمي أنظمة معينة من الذكاء الاصطناعي"، والذي يُفهَم منه أن هناك التزامات خاصة بالشفافية لبعض أنظمة الذكاء الاصطناعي. فليس معنى ذلك أن هذه الالتزامات هي الوحيدة التي تطبق على تقنية التزييف العميق، ولكن معنى ذلك أن القانون يضفي التزاماً إضافياً خاصاً لهذه التقنية دون غيرها من تقنيات الذكاء الاصطناعي نظراً

[١] انظر في ذلك:

Mateusz Łabuz, Regulating Deep Fakes in the Artificial Intelligence Act, ACIG, vol. 2, no. 1, 2023, p. 12, available at: https://shorturl.at/dJWxh [Accessed: 20 August 2024]

لطبيعتها الخاصة. وبذلك فلا يوجد ما يمنع من اعتبار التزييف العميق من قبيل الأنظمة عالية الخطورة، كما يطبق عليه الالتزامات الخاصة بالشفافية.

ثالثاً: أن المفوضية الأوروبية، في مقترح القانون، أشارت في الفقرة ٣٨ من قانون الذكاء الاصطناعي، التي سردت بعض الأنظمة عالية الخطورة، إلى أنه: نظرًا لطبيعة الأنشطة المعنية والمخاطر المرتبطة بها، يجب أن تشمل أنظمة الذكاء الاصطناعي عالية الخطورة على وجه الخصوص أنظمة الذكاء الاصطناعي المُخصَصة لاستخدامها من قبل سلطات إنفاذ القانون (...) للكشف عن "التزييف العميق". كما تضمن هذا المقترح أنظمة الذكاء الاصطناعي المُخصصَة لاستخدامها من قبل سلطات إنفاذ القانون للكشف عن التزييف العميق في قائمة أنظمة الذكاء الاصطناعي عالية المخاطر في الملحق الثالث[١]، إلا أن البرلمان الأوروبي قد حذف هذا الجزء الخاص بالكشف عن التزييف العميق من الفقرة رقم ٣٨ وكذلك من الملحق الثالث[٢].

---

[١] انظر في ذلك:

European Commission, Proposal for Regulation of the European Parliament and the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts. COM (2021) 206 final. 2021, para. 38. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206 [Accessed: 20 August 2024]

[٢] انظر في ذلك:

European Parliament, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. (COM 2021)0206 – C9-0146/2021 – 2021/0106(COD))1. P9_TA (2023)0236. 2023. Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html [Accessed: 20 August 2024].

وعلى الرغم من أن هذا النص خاص بالـ "الكشف عن التزييف العميق" وليس فعل التزييف العميق نفسه، إلا أنه يثبت وجهة نظر الباحث في أن التزييف العميق بشكل عام قد يكون من قبيل الأفعال عالية الخطورة، وبذلك جاء النص في الصياغة النهائية على أنه يعتبر من قبيل الأنظمة عالية الخطورة: "(ج) أنظمة الذكاء الاصطناعي المخصصة للاستخدام من قبل سلطات إنفاذ القانون أو نيابة عنها، أو من قبل مؤسسات أو هيئات أو مكاتب أو وكالات الاتحاد، لدعم سلطات إنفاذ القانون لتقييم موثوقية الأدلة في سياق التحقيق أو مقاضاة الجرائم الجنائية"[١]. وهو بذلك نص عام يمكن أن يتسع ليشمل أنظمة الكشف عن التزييف العميق وغيرها. وبالتالي كان ذكره في المقترح تزيُداً دون مبرر. وعلى الرغم من محاولة البعض الإشارة إلى أنه كان بهدف إضافة قيود على تصرفات الدولة وحماية لحقوق الأفراد إلا أنه رأي لم يكتب له القبول نظراً لأهمية دور الدولة في مواجهة هذه التقنية والحاجة إلى بذلها مجهود أكبر للسيطرة على هذه التقنية[٢].

كما يؤكد الخبراء باستمرار على أهمية أدوات الكشف عن التزييف العميق لمكافحة الممارسات الضارة لهذه التقنية، وتعزيز قدرة سلطات إنفاذ القانون، وتوفير الحماية للإجراءات القضائية. ومن المحتمل أن يكون لهذه الأدوات دورًا متزايد الأهمية في مواجهة الزيادة في الجرائم التي تنطوي على

---

[١] انظر في ذلك:

ANNEX III of the EU AI Act.

[٢] انظر في ذلك:

Cristina Mesa, Deep fakes: the media and the legal system is under threat, 2023, available at: https://shorturl.at/171b4 [Accessed: 22 August 2024].

الاستخدام الضار للتزييف العميق مثل الابتزاز، وانتحال الشخصية، والاحتيال المالي، وتزوير الأدلة[١].

رابعاً: افتراض أن أفعال التزييف العميق تتطلب فقط التزاماً بالشفافية هو افتراض يجهل قدرات هذه التقنية وما يمكن أن تحققه من نتائج، فهذه التقنية تحتوي على قدرات تمكن من التلاعب بالمحتوى السمعي والبصري بما قد يؤدي إلى أضرار وخيمة، بدايةً من خداع مجموعة أشخاص لأهداف النصب أو التدليس، ووصولاً إلى تحقيق أضرار ماسة بالأمن القومي للدول على نحو ما أشرنا سابقاً[٢].

كما أشارت نتائج الاختبارات التي أجراها مجموعة من العلماء حول الاستخدامات الضارة للتزييف العميق إلى أن التلاعب قد يُظهِر مستوي مختلف من الخطورة، وأن مستوى الخطورة يعتمد بشكل كبير على نوع التطبيقات المحددة ويعتمد إلى حد ما على حالة الاستخدام الفعلية؛ أي أن خطورة التزييف العميق يحددها مجموعة معايير تتعلق في المقام الأول بالأغراض المختلفة وراء إنشاءه ونشره والسياق المستخدم فيه[٣]. وبذلك، كما أشار البعض، فإن بعض عمليات

---

[١] انظر في ذلك:

Mateusz Łabuz, Regulating Deep Fakes in the Artificial Intelligence Act, Op. cit., p. 14.

[٢] انظر في ذلك:

Matúš Mesarčík et al., Stance on The Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence – Artificial Intelligence Act, Kempelen Institute of Intelligent Technologies, 2021, p. 6, available at: https://zenodo.org/doi/10.5281/zenodo.12567879 [Accessed: 21 August 2024]

[٣] انظر في ذلك:

Centre for Digital Governance, The false promise of transparent deep fakes: How transparency obligations in the draft AI Act fail to deal with the threat of disinformation and image-based sexual abuse, Hertie

التزييف العميق ستكون عالية الخطورة، في حين أن البعض الآخر قد يكون غير ضار تمامًا[١].

ويؤيد ذلك أيضاً ما أشار إليه المجلس الاتحادي الألماني باعتباره أحد المجالس البرلمانية القليلة في أوروبا التي اهتمت بمسألة التزييف العميق بشكل مباشر، وتم التأكيد على أن التزييف العميق يمكن أن يتلاعب بالخطاب العام، وبالتالي يمارس تأثيرًا كبيرًا على تشكيل الرأي العام. وبذلك لا ينبغي التعامل معه كأثر جانبي لاستخدام أنظمة الذكاء الاصطناعي، واقترح النظر إلى التزييف العميق باعتباره نظام ذكاء اصطناعي عالي الخطورة[٢].

وبذلك يجب النظر إلى التزييف العميق بما قد يترتب على استخدامه من تدمير لعالم المعلومات ومن ضياع للثقة في أي محتوى سمعي وبصري، وما قد ينتج عن ذلك من أفعال ذات أضرار كبيرة كالتلاعب في عمليات الانتخابات، أو التلاعب بالبيانات الخاصة بأمن الدول سواء السياسية أو الاقتصادية أو العسكرية. فعلى سبيل المثال قد يتم استخدام هذه التقنية لإنشاء محتوى عن تفجيرات إرهابية في دولة معينة بما قد يؤدي إلى انهيار البورصة

School, 2022. Available at: https://rb.gy/m0nm7c [Accessed: 21 August 2024]

[١] انظر في ذلك:

Rüya Tuna Toparlak, "Criminalising Pornographic Deep Fakes: A Gender-Specific Inspection of Image-Based Sexual Abuse," SciencesPo Law School The 10th Graduate Conference, 2022, pp. 11-15, available at: https://rb.gy/mnsnpn [Accessed: 21 August 2024]

[٢] انظر في ذلك:

Bundesrat (Federal Council), Resolution of the Federal Council. Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legal acts, 2021, available: Microsoft Word - Vorblatt 210468-0 (bundesrat.de) [Accessed: 22 August 2024]

وإثارة الفزع والخوف بين المواطنين، وهو ما حدث بالفعل كما سبق أن ذكرنا. وبذلك فالعوامل المحيطة بفعل التزييف العميق مثل الغرض من الانشاء والسياق المستخدم فيه والضرر المتوقع هي ما تحدد معيار خطورته.

وبالنظر إلى الملحق الثالث للقانون (ANNEX III) نجد أنه شمل ثمانِ قطاعات اعتبرها المشرع عالية الخطورة، وهي القياسات الحيوية (Biometrics)، والبنية الأساسية الحيوية (الحرجة)، والتعليم، والتوظيف، والوصول إلى الخدمات الخاصة الأساسية والخدمات والمزايا العامة الأساسية، ومجال انفاذ القانون، وإدارة العدالة، والهجرة واللجوء[١]. وبالتبعية يمكننا استنتاج أنه متى تم استخدام التزييف العميق –كأحد أنظمة الذكاء الاصطناعي– في هذه القطاعات فقد يمكن اعتباره من الأفعال عالية الخطورة.

وهذه القطاعات هي قطاعات جوهرية لأمن الدول والمجتمعات، فقد تستخدم أنظمة الذكاء الاصطناعي للتحكم في توزيع الطاقة وإمدادات المياه وشبكات الاتصالات، أو التشخيص الطبي وتوصيات العلاج ومراقبة رعاية المرضى، أو المركبات ذاتية القيادة، أو أنظمة إدارة حركة المرور.

وبالنظر إلى التزييف العميق نجد أنه قد يُستخدَم في بعض هذه القطاعات، والتي من أهمها قطاع التعليم. وحيث أن المشرع ارتأى أن أنظمة الذكاء الاصطناعي في مجال التعليم عالية الخطورة كما هو وارد في الملحق الثالث من القانون، وذلك في حال استخدام هذه الأنظمة للوصول أو القبول أو تعيين الأشخاص الطبيعيين في المؤسسات التعليمية والتدريب المهني على جميع

---

[١] انظر في ذلك:

ANNEX III of the EU AI Act, Op. Cit.

المستويات[١]، فإنه متى تم استخدام التزييف العميق في هذا السياق فإنه يمكن اعتباره من قبيل الأنظمة عالية الخطورة وفقاً للمادة السادسة من القانون.

كما تضمّن الملحق الثالث أنظمة الذكاء الاصطناعي المتعلقة بإدارة العدالة والعملية الديمقراطية تعتبر أنظمة عالية الخطورة، وبالتطبيق على التزييف العميق فإذا تم استخدامه للتأثير على نتائج الانتخابات أو الاستفتاءات أو سلوك التصويت للأشخاص الطبيعيين أثناء ممارسة حقهم في التصويت في الانتخابات أو الاستفتاءات يمكننا اعتباره من الأنظمة عالية الخطورة. إلا أن ذلك لا يشمل أنظمة الذكاء الاصطناعي التي لا يتعرض الأشخاص الطبيعيون لمخرجاتها بشكل مباشر، مثل الأدوات المستخدمة في تنظيم الحملات السياسية أو تحسينها أو هيكلتها من وجهة نظر إدارية أو لوجستية[٢].

وبذلك متى تم استخدام التزييف العميق في القطاعات الواردة في الملحق الثالث للقانون يمكن اعتباره من الأنظمة عالية الخطورة، ولكن هل الوصول إلى هذه النتيجة يعنى أن أي استخدام لأنظمة الذكاء الاصطناعي، وتحديداً التزييف العميق، في هذه القطاعات قد يصنفها على أنها عالية الخطورة أما أن هناك شروطاً معينة يجب توافرها لتحقق هذه النتيجة؟

تناولت الفقرة الثالثة من المادة السادسة[٣] من القانون هذا التساؤل، فنصت على أنه لا يُعتبر نظام الذكاء الاصطناعي المُشَار إليه في الملحق

---

[١] انظر في ذلك:

Paragraph 3 of the ANNEX III of the EU AI Act.

[٢] انظر في ذلك:

Paragraph 8 of the ANNEX III of the EU AI Act.

[٣] انظر في ذلك:

الثالث عالي الخطورة إذا لم يشكل خطرًا كبيرًا على صحة الأشخاص الطبيعيين أو سلامتهم أو حقوقهم الأساسية، بما لا يؤثر بشكل ملموس على نتيجة اتخاذ القرار، وحددت أربع حالات يتحقق فيها ذلك، وهي:

الحالة الأولى: المهام الإجرائية المحدودة: وتشمل أنظمة الذكاء الاصطناعي التي تؤدي مهام إجرائية محدودة مع الحد الأدنى من التأثير على النتائج. ومن أمثلة ذلك – كما ذكرت ديباجة القانون – نظام الذكاء الاصطناعي الذي يحول البيانات غير المنظمة إلى بيانات منظمة، أو نظام الذكاء الاصطناعي الذي يصنف المستندات الواردة إلى فئات، أو نظام الذكاء الاصطناعي المُستخدَم للكشف عن التكرارات بين عدد كبير من التطبيقات. هذه المهام ذات طبيعة ضيقة ومحدودة بحيث لا تشكل سوى مخاطر محدودة، لا

Paragraph 3 of Article 6 of the EU AI Act. It provides that "…….. an AI system referred to in Annex III shall not be considered to be high-risk where it does not pose a significant risk of harm to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making. The first subparagraph shall apply where any of the following conditions is fulfilled:
(a) the AI system is intended to perform a narrow procedural task;
(b) the AI system is intended to improve the result of a previously completed human activity;
(c) the AI system is intended to detect decision-making patterns or deviations from prior decision-making patterns and is not meant to replace or influence the previously completed human assessment, without proper human review; or
(d) the AI system is intended to perform a preparatory task to an assessment relevant for the purposes of the use cases listed in Annex III".

تزداد من خلال استخدام نظام الذكاء الاصطناعي في سياق مُدَرج كاستخدام عالي الخطورة في ملحق لهذه اللائحة[١].

الحالة الثانية: تحسين نتائج الأنشطة البشرية المكتملة سابقًا: وتشمل أنظمة الذكاء الاصطناعي التي تعمل على تعزيز المهام البشرية الحالية دون تغيير القرارات النهائية. ويحدث ذلك في الحالة التي تقتصر فيها المهمة التي يؤديها نظام الذكاء الاصطناعي تهدف إلى تحسين نتيجة نشاط بشري مكتمل سابقًا. وينطبق ذلك، على سبيل المثال، على أنظمة الذكاء الاصطناعي التي تهدف إلى تحسين اللغة المستخدمة في المستندات التي تم صياغتها مسبقًا. على سبيل المثال، الأنظمة المتعلقة بالأسلوب الأكاديمي للغة، أو الأنظمة المستخدمة لمحاذاة النص مع رسالة علامة تجارية معينة[٢].

الحالة الثالثة: اكتشاف أنماط اتخاذ القرار دون التأثير على النتائج: وتشمل أنظمة الذكاء الاصطناعي التي تعمل على تحليل أنماط اتخاذ القرارات دون التأثير المباشر على القرارات. فقد يكون الهدف من نظام الذكاء الاصطناعي اكتشاف أنماط صنع القرار، أو الكشف عن الانحرافات في أنماط صنع القرار السابقة. وتشمل أنظمة الذكاء الاصطناعي هذه، على سبيل المثال، تلك التي يمكن استخدامها لتحديد نمط تصنيف معين من المعلم في المجال

---

[١] الفقرة ٥٣ من ديباجة قانون الذكاء الاصطناعي الاتحاد الأوروبي.

[٢] انظر في ذلك:

Ibid.

التعليمي للتحقق بعد ذلك مما إذا كان المعلم قد انحرف عن نمط التصنيف بغرض تحديد التناقضات أو الشذوذ المحتمل[١].

الحالة الرابعة: المهام التحضيرية للتقييمات: ويقصد بها أنظمة الذكاء الاصطناعي التي تقوم بالمهام التحضيرية للتقييمات دون السلطة المباشرة لاتخاذ القرار. وتغطي هذه الحالة، من بين أمور أخرى، الحلول الذكية للتعامل مع الملفات، والتي تتضمن وظائف مختلفة من الفهرسة والبحث ومعالجة النصوص والكلمات أو ربط البيانات بمصادر بيانات أخرى، أو أنظمة الذكاء الاصطناعي المستخدمة لترجمة المستندات الأولية[٢].

وعلى ذلك فإن أنظمة الذكاء الاصطناعي في الحالات السابقة لا تعتبر من قبيل الأنظمة عالية الخطورة، حتى لو حدثت في القطاعات الواردة التي نص عليها القانون في الملحق الثالث. وبالتالي لا يمكن تصنيف التزييف العميق الذي يمكن استخدامه في هذه الحالات على أنه نظام عالي الخطورة. وبطبيعة الحال فإن الأمر سيتوقف على كل حالة على حده لتصنيف فعل التزييف العميق، يتم فيها دراسة السياق والظروف التي حدث فيها والنتائج المترتبة على الفعل لتصنيفه بشكل مناسب وفقاً للقانون.

ومتى ثبت أن التزييف العميق ضمن الأنظمة عالية الخطورة، فإن مقدم الخدمة يقع على عاتقه عدة التزامات حدّدها القانون في العديد من المواد، وهذه الالتزامات هي:

---

[١] انظر في ذلك:

Ibid.

[٢] انظر في ذلك:

Ibid.

أولاً: تطبيق نظام إدارة المخاطر (المادة ٩) ونظام إدارة الجودة (المادة ١٧):

نصت المادة ٩ من القانون على ما يسمى بـ"نظام إدارة المخاطر" والذي يلتزم مقدم أنظمة الذكاء الاصطناعي بتنفيذه، وهو نظام يشمل تحديد وتحليل المخاطر المعروفة والمتوقعة بشكل معقول والتي يمكن أن يفرضها نظام الذكاء الاصطناعي على الصحة أو السلامة أو الحقوق الأساسية عند استخدامه وفقًا للغرض المقصود منه؛ وكذا تقدير وتقييم المخاطر التي قد تنشأ عند استخدام نظام الذكاء الاصطناعي وفقًا للغرض المقصود منه، وفي ظل ظروف سوء الاستخدام المتوقعة بشكل معقول؛ وتقييم المخاطر الأخرى التي قد تنشأ، وذلك بناءً على تحليل البيانات التي تم جمعها من نظام مراقبة ما بعد التسويق؛ واعتماد تدابير إدارة المخاطر المناسبة والمستهدفة والمُصمَمة لمعالجة المخاطر المعروفة والمتوقعة بشكل معقول بعد اختبارها، وهي عملية متكررة ومستمرة يتم تشغيلها طوال دورة حياة نظام الذكاء الاصطناعي بالكامل[١].

كما يجب تطبيق ما يسمى بـ "نظام إدارة الجودة" لضمان الامتثال لهذه اللائحة. يجب توثيق هذا النظان بطريقة منهجية ومنظمة في شكل سياسات وإجراءات وتعليمات مكتوبة. ويشمل الجوانب التالية: استراتيجية الامتثال التنظيمي؛ والتقنيات والإجراءات المنهجية التي يجب استخدامها لتصميم نظام الذكاء الاصطناعي والتحكم في تصميمه والتحقق من هذا التصميم؛ والمواصفات الفنية التي يجب تطبيقها. وفي حالة عدم تطبيق المعايير ذات الصلة بالكامل أو عدم تغطيتها لجميع المتطلبات المعمول بها، يتم تحديد الوسائل التي يجب استخدامها لضمان امتثال نظام الذكاء الاصطناعي لتلك المتطلبات. ويشمل

[١] المادة ٩ من قانون الذكاء الاصطناعي الصادر من الاتحاد الأوروبي.

أيضاً أنظمة وإجراءات إدارة البيانات، بما في ذلك الحصول على البيانات وجمعها وتحليلها ووضع علامات عليها وتخزينها وتصفية البيانات واستخراج البيانات وتجميع البيانات والاحتفاظ بالبيانات وأي عملية أخرى تتعلق بالبيانات يتم إجراؤها قبل ولغرض طرح نظام الذكاء الاصطناعي في سوق الاتحاد الأوروبي[١].

ثانياً: تنفيذ ممارسات حوكمة البيانات وإدارتها للتدريب والتحقق واختبار البيانات (المادة ١٠):

ويشمل هذا الالتزام تغطية الممارسات الخاصة بعمليات جمع البيانات ومصدرها؛ وعمليات معالجة إعداد البيانات ذات الصلة؛ وتقييم مدى توفر وكمية وملاءمة مجموعات البيانات المطلوبة؛ وفحص التحيزات المحتملة التي من المرجح أن تؤثر على صحة وسلامة الأفراد أو التي يكون لها تأثير سلبي على الحقوق الأساسية أو تؤدي إلى تمييز محظور، وخاصة عندما تؤثر مخرجات البيانات على المدخلات للعمليات المستقبلية. كما يتضمن هذه الالتزام تحديد ثغرات أو أوجه القصور في البيانات ذات الصلة التي تمنع الامتثال لقانون الذكاء الاصطناعي للاتحاد الأوروبي، وكيف يمكن معالجتها[٢].

ثالثاً: تصميم نظام الذكاء الاصطناعي لضمان أن يكون تشغيله بدرجة كافية من الشفافية لتمكين المستخدمين من تفسير مخرجاته واستخدامه بشكل مناسب وصياغة تعليمات الاستخدام (المادة ١٣):

---

[١] المادة ١٧ من قانون الذكاء الاصطناعي الصادر من الاتحاد الأوروبي.

.

[٢] المادة ١٠ من قانون الذكاء الاصطناعي الصادر من الاتحاد الأوروبي.

فيجب أن تحتوي تعليمات الاستخدام على الأقل على هوية وتفاصيل الاتصال الخاصة بمُقدِم الخدمة؛ وخصائص وقدرات وقيود أداء نظام الذكاء الاصطناعي؛ وأي ظروف معروفة ومتوقعة قد يكون لها تأثير على هذا المستوى المتوقع من الدقة والأمن السيبراني؛ وأي ظروف معروفة أو متوقعة، تتعلق باستخدامه وفقًا للغرض المقصود منه والتي قد تؤدي إلى مخاطر على الصحة والسلامة أو الحقوق الأساسية. ويشمل كذلك التغييرات التي تطرأ على نظام الذكاء الاصطناعي وأدائه والتي تم تحديدها مسبقًا في لحظة تقييم المطابقة الأولي؛ وتدابير الرقابة البشرية التي تم تنفيذها (بما في ذلك التدابير الفنية الموضوعة لتسهيل تفسير مخرجات نظام الذكاء الاصطناعي من قبل المستخدمين)؛ والموارد الحسابية والأجهزة اللازمة. ويتضمن أيضاً تحديد العمر المتوقع لنظام الذكاء الاصطناعي، وأي تدابير صيانة ورعاية ضرورية لضمان الأداء السليم لنظام الذكاء الاصطناعي (بما في ذلك تحديثات البرامج)؛ وأخيراً وصف للآليات المضمنة في نظام الذكاء الاصطناعي والتي تسمح للمستخدمين بجمع السجلات وتخزينها وتفسيرها بشكل صحيح[١].

رابعاً: تصميم نظام الذكاء الاصطناعي لضمان الرقابة البشرية الفعالة عند الاستخدام من أجل منع او تقليل المخاطر على الصحة أو السلامة أو الحقوق الأساسية (المادة ١٤):

ويتحقق ذلك من خلال تنفيذ التدابير المُضمَنة في نظام الذكاء الاصطناعي من قبل مُقدِم الخدمة، بغرض فهم القدرات والقيود ذات الصلة بنظام الذكاء الاصطناعي بشكل صحيح، والقدرة على مراقبة تشغيله بشكل فعال. كما يجب البقاء على دراية بالتوجه المحتمل للاعتماد تلقائيًا أو الاعتماد

[١] المادة ١٣ من قانون الذكاء الاصطناعي الصادر من الاتحاد الأوروبي.

المفرط على الناتج الذي ينتجه نظام الذكاء الاصطناعي؛ والقدرة على اتخاذ قرار، في أي موقف معين، بعدم استخدام نظام الذكاء الاصطناعي، أو تجاهل ناتجه، أو تجاوزه، أو عكسه. ويجب أيضاً أن يتاح التدخل في تشغيل نظام الذكاء الاصطناعي، أو مقاطعته من خلال زر "إيقاف"، أو اتخاذ أي إجراء مماثل يمكن النظام من التوقف بطريقة آمنة[١].

خامساً: تصميم وتنفيذ التدابير الفنية والتنظيمية لضمان تحقيق نظام الذكاء الاصطناعي لمستوى مناسب من الدقة والمتانة والأمن السيبراني طوال دورة حياته:

ويتم تنفيذ هذا الالتزام من خلال اتخاذ التدابير الفنية والتنظيمية من أجل ضمان أن يكون نظام الذكاء الاصطناعي مرنًا قدر الإمكان فيما يتعلق بالأخطاء أو العيوب أو التناقضات التي قد تحدث داخل النظام أو البيئة التي يعمل فيها، وخاصةً بسبب تفاعله مع الأفراد أو الأنظمة الأخرى. وكذلك محاولة القضاء على أو تقليل خطر المخرجات المتحيزة التي قد تؤثر على المدخلات للعمليات المستقبلية قدر الإمكان، بالإضافة إلى ضمان المرونة ضد محاولات الغير غير المصرح لهم لتغيير استخدام النظام أو مخرجاته أو أدائه من خلال استغلال نقاط ضعف النظام[٢].

سادساً: الاحتفاظ بالوثائق، تحت تصرف السلطات الوطنية المختصة، لمدة ١٠ سنوات بعد طرح نظام الذكاء الاصطناعي في سوق الاتحاد الأوروبي أو وضعه في الخدمة (المادة ١٨):

---

[١] المادة ١٤ من قانون الذكاء الاصطناعي الصادر من الاتحاد الأوروبي.

[٢] المادة ١٥ من قانون الذكاء الاصطناعي الصادر من الاتحاد الأوروبي.

يتضمن ذلك الاحتفاظ بالوثائق الفنية؛ والوثائق المتعلقة بنظام إدارة الجودة؛ والوثائق المتعلقة بالتغييرات التي وافقت عليها الهيئات المخطرة، حيثما ينطبق ذلك؛ والقرارات والوثائق الأخرى الصادرة عن الهيئات المخطرة، حيثما ينطبق ذلك؛ وإعلان المطابقة للاتحاد الأوروبي[١].

سابعاً: الاحتفاظ بالسجلات التي يتم إنشاؤها تلقائيًا لمدة لا تقل عن ٦ أشهر (المادة ١٩) وإبلاغ أصحاب المصلحة المعنيين وتنفيذ الإجراءات التصحيحية في حالة عدم المطابقة أو المخاطر (المادة ٢٠)، والتسجيل في قاعدة بيانات الاتحاد الأوروبي (المادة ٤٩)، والإبلاغ عن الحوادث الخطيرة إلى سلطات مراقبة السوق الوطنية والتحقيق فيها (المادة ٧٣).

وقد تضمنت المادة ٤/٩٩ من القانون عقوبة عدم الامتثال للالتزامات المنصوص عليها فيما يتعلق بالأنظمة عالية الخطورة، والتي قد تخضع لغرامات إدارية تصل إلى ١٥ مليون يورو أو، إذا كان الجاني مؤسسة، تصل إلى ٣٪ من إجمالي مبيعاتها السنوية على مستوى العالم للسنة المالية السابقة، أيهما أعلى[٢].

[١] المادة ١٨ من قانون الذكاء الاصطناعي الصادر من الاتحاد الأوروبي.

[٢] المادة ٤/٩٩ من قانون الذكاء الاصطناعي الصادر من الاتحاد الأوروبي.

المطلب الثالث

تطبيق الالتزام بالشفافية والتمييز على التزييف العميق

أشارت لجنة الشؤون القانونية في البرلمان الأوروبي، في بداية عام ٢٠٢١، إلى أن عمليات التزييف العميق يجب أن تكون مشمولة بشكل عام بقواعد الإفصاح، نظراً لإمكانية استخدامها للابتزاز، أو إنتاج تقارير اخبارية كاذبة، أو ضياع ثقة الجمهور والتأثير على الخطاب العام. ومثل هذه الممارسات لديها القدرة على زعزعة استقرار البلدان، ونشر المعلومات المضللة والتأثير على الانتخابات[١].

وقد أشرنا سابقاً إلى أن هناك من يرى أن التزييف العميق يتطلب التزاماً بالشفافية فقط على النحو الوارد بالقانون، بينما نؤيد رأيًا آخر يعتبر أن للتزييف العميق طبيعة خاصة، ولا يوجد ما يمنع من إضافة الالتزام بالشفافية إلى جانب اعتباره نظامًا عالي الخطورة في بعض الحالات. ويؤكد ذلك ما اقترحته المفوضية، في البداية، من تصنيف عمليات التزييف العميق على أنها أنظمة تتطلب مراعاة الحد الأدنى من الشفافية[٢]، إلا أن هذا الاقتراح أثار جدلاً مبررًا

---

[١] انظر في ذلك:

European Parliament›s Committee on Legal Affairs, Report on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice. 2020/2013(INI). 2021, available at: https://www.europarl.europa.eu/doceo/document/A-9-2021-0001_EN.html [Accessed: 26 August 2024]

[٢] انظر في ذلك:

European Commission, Proposal for Regulation of the European Parliament and the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union

بسبب التهديدات المرتبطة بوجود عمليات التزييف العميق في مجال المعلومات وبالتالي عدم كفاية الالتزام بالشفافية للحد من هذه التهديدات. ونتيجة لذلك، لم يظهر هذا الاقتراح في الصياغة النهائية للقانون[١]، مما يؤكد ما سبق وأن أشرنا إليه من عدم الاكتفاء بالالتزام بالشفافية لتنظيم تقنية التزييف العميق.

فقد نصت المادة ٥٠ المتعلقة بالتزامات الشفافية لمُقدِمي ومُستخدِمي أنظمة معينة من أنظمة الذكاء الاصطناعي في الفقرة الرابعة على أنه "..٤- يتعين على مُستخدِمي نظام الذكاء الاصطناعي الذين يُنشئون أو يتلاعبون بمحتوى الصور أو الصوت أو الفيديو الذي يشكل تزييفًا عميقًا، أن يكشفوا أن المحتوى قد تم إنشاؤه أو التلاعب به بشكل مصطنع. ولا ينطبق هذا الالتزام عندما يكون الاستخدام مُصرَحًا به بموجب القانون للكشف عن جريمة جنائية أو منعها أو التحقيق فيها أو مقاضاة مرتكبيها، أو عندما يشكل المحتوى جزءًا من عمل، أو برنامج فني، أو إبداعي، أو ساخر، أو خيالي، أو مشابه بشكل واضح. وبالتالي، فإن التزامات الشفافية المنصوص عليها في هذه الفقرة تقتصر على الكشف عن وجود مثل هذا المحتوى المزيف بطريقة مناسبة لا تعيق عرض العمل أو الاستمتاع به"[٢].

---

legislative acts. COM (2021) 206 final, 2021, available at: https://shorturl.at/UCaMl [Accessed: 26 August 2024]

[١] انظر في ذلك:

M Matúš Mesarčík et al., Stance on The Proposal for a Regulation, Op. cit., pp. 7-8.

[٢] انظر في ذلك: الفقرة ٤ من المادة ٥٠ من قانون الذكاء الاصطناعي الصادر من الاتحاد الأوروبي والتي تنص على:

"Deployers of an AI system that generates or manipulates image, audio or video content constituting a deep fake, shall disclose that the

والحقيقة أن الالتزام بالشفافية لم يظهر للمرة الأولى في قانون الذكاء الاصطناعي، فقد أشارت مجموعة المبادئ التوجيهية الأخلاقية لعام ٢٠١٩ للذكاء الاصطناعي، التي طوّرتها مجموعة الخبراء العليا المستقلة للذكاء الاصطناعي المشكلة من المفوضية الأوروبية، إلى سبعة مبادئ للذكاء الاصطناعي تهدف إلى المساعدة في ضمان أن يكون الذكاء الاصطناعي جديرًا بالثقة وسليمًا من الناحية الأخلاقية. وقد شملت هذه المجموعة الالتزام بالشفافية كأحد أهم هذه المبادئ[١].

وعند محاولة تحديد معنى الشفافية، نجد أن الفقرة ٢٧ من ديباجة القانون أشارت إلى أن "الشفافية تعني أن يتم تطوير أنظمة الذكاء الاصطناعي واستخدامها بطريقة تسمح بإمكانية التتبع والتفسير بشكل مناسب، مع جعل البشر على دراية بأنهم يتواصلون أو يتفاعلون مع نظام الذكاء الاصطناعي، بالإضافة إلى إبلاغ المستخدمين بشكل مناسب بقدرات وحدود نظام الذكاء الاصطناعي والأشخاص المتأثرين بحقوقهم"[٢].

---

content has been artificially generated or manipulated. This obligation shall not apply where the use is authorised by law to detect, prevent, investigate or prosecute criminal offence. Where the content forms part of an evidently artistic, creative, satirical, fictional or analogous work or programme, the transparency obligations set out in this paragraph are limited to disclosure of the existence of such generated or manipulated content in an appropriate manner that does not hamper the display or enjoyment of the work".

[١] انظر في ذلك:
The European Commission, High-Level Expert Group on Artificial Intelligence, ETHICS GUIDELINES FOR TRUSTWORTHY AI, 8 April 2019, p. 14, available at: https://shorturl.at/6aqBc [Accessed: 27 August 2024]

[٢] انظر في ذلك: الفقرة ٢٧ من ديباجة قانون الذكاء الاصطناعي الصادر من الاتحاد الأوروبي.

ووفقًا لهذا الوصف، فإن إحدى الأولويات الرئيسية لقانون الذكاء الاصطناعي في الاتحاد الأوروبي هو إنشاء نظام موثوق يتميز بالشافية لأنظمة الذكاء الاصطناعي، وهو أمر أساسي في تمكين مُشغِلي السوق وكذلك الأفراد من فهم تصميم أنظمة الذكاء الاصطناعي واستخدامها. وهو أمر بالغ الأهمية أيضًا لتعزيز التطوير والاستخدام المسؤول للذكاء الاصطناعي، وتعزيز مساءلة الجهات الفاعلة ذات الصلة في السوق عن عمليات الذكاء الاصطناعي الخاصة بهم.

وتجدر الإشارة إلى أن المادة ٤/٥٠ من قانون الذكاء الاصطناعي أدرجت الالتزام بالشفافية ليكون منطبقًا على أنظمة محددة على سبيل الحصر. فألزمت المستخدمين (Deployers) أن يكشفوا للأفراد أن المحتوى تم إنتاجه أو تعديله بشكل مصطنع، واستثنت من ذلك:

أولاً: أنظمة الذكاء الاصطناعي المصرح بها لأغراض إنفاذ القانون وذلك بهدف الكشف عن جريمة جنائية أو منعها أو التحقيق فيها أو مقاضاة مرتكبيها؛

ثانياً: الأعمال الفنية أو الإبداعية التي لا تعيق الشفافية الاستمتاع بها، وذلك في الحالة التي يشكل فيها المحتوى جزءًا من عمل أو برنامج فني أو إبداعي، حيث تقتصر التزامات الشفافية على الكشف عن وجود مثل هذا المحتوى المزيف بطريقة لا تعيق عرض العمل أو الاستمتاع به.

"Transparency means that AI systems are developed and used in a way that allows appropriate traceability and explainability, while making humans aware that they communicate or interact with an AI system, as well as duly informing deployers of the capabilities and limitations of that AI system and affected persons about their rights."

ويعتبر هذا الالتزام هو الالتزام الوحيد الذي أورده المشرع صراحةً فيما يتعلق بالتزييف العميق، وذلك بغض النظر عن شدته أو خطورته أو السياق المستخدم فيه. وهو بذلك يختلف عن الالتزام بالشفافية الذي ينطبق فقط على الأنظمة عالية الخطورة الوارد في المادة ١٣ من القانون والتي نصت على أنه "يجب تصميم وتطوير أنظمة الذكاء الاصطناعي عالية المخاطر بطريقة تضمن أن يكون تشغيلها بدرجة كافية من الشفافية لتمكين المستخدمين من تفسير مخرجات النظام واستخدامه بشكل مناسب...."[١].

وبذلك تختلف متطلبات الشفافية بموجب قانون الذكاء الاصطناعي للاتحاد الأوروبي لنظام ذكاء اصطناعي معين وفقًا لمستوى الخطورة في النظام. ويتحدد بناءً عليه القواعد المطبقة على أساس كل حالة على حدة بعد إجراء فحص دقيق ومراعاة الظروف الخاصة. إلا أن القانون لم يتناول بوضوح المستوى الفعلي للشفافية والقدرة على الفهم المطلوبين لأنظمة الذكاء الاصطناعي. بعبارة أخرى، ليس من الواضح بعد من الناحية العملية كيف وإلى أي مدى سيكون الامتثال لقواعد قانون الذكاء الاصطناعي للاتحاد الأوروبي بشأن الشفافية كافياً، وهو ما قد يتضح عند تطبيق القانون.

ويجب الإشارة إلى أنه على الرغم من أن معظم عمليات التلاعب والتزييف تصدر من جهات داخلية، إلا أنه لا يمكن استبعاد تأثير الجهات الفاعلة الخارجية، بما في ذلك الدول الأجنبية، في المسائل ذات الطبيعة السياسية البحتة. ويتضاعف انتشار المحتوى وتأثيره بشكل عام من خلال الرغبة العامة في مشاركته، وهو ما يعكس أنماط نشر المعلومات المضللة بسبب ضخ

[١] المادة ١٣ من قانون الذكاء الاصطناعي الصادر من الاتحاد الأوروبي.

"معلومات كاذبة، ولكنها مقنعة في بيئة جاهزة وراغبة في مشاركة المعلومات" من قبل المستخدمين العاديين[١].

ونظرًا لأن بعض عمليات التزييف العميق يتم إنشاؤها لأغراض التلاعب بالمعلومات والتدخل فيها، فيجب افتراض أن الجهات الفاعلة الحكومية وغير الحكومية المشاركة في هذه الممارسة قد لا تمتثل لأي التزامات بالشفافية. وفي هذا السياق، ستكون الحلول التقنية البسيطة القائمة على الإفصاح عديمة الجدوى[٢]. وأمام هذا التجاهل لخصوصية إنشاء ونشر التزييف العميق، وسياق السياسة الدولية وأنماط التضليل المعروفة بالفعل، فإن التزامات الشفافية ستكون قابلة للتطبيق على جزء صغير فقط من أفعال التزييف العميق"[٣].

وقد انتقد البعض استخدام القانون في الفقرة الرابعة من المادة ٥٠ لمصطلح "المستخدمين" (Deployers) واستبعاد مُقدِمي الخدمة(providers).

---

[١] انظر في ذلك:

Danielle K. Citron and Robert Chesney, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," California Law Review, vol. 107, no. 18, pp. 1753–1820, 2019, p. 1767, available at: https://shorturl.at/Q1Ygg [Accessed: 26 August 2024]

[٢] انظر في ذلك:

Joshua Habgood-Coote, Deepfakes and the epistemic apocalypse, Synthese, vol. 201, no. 3, 2023, p. 14, available at: https://link.springer.com/article/10.1007/s11229-023-04097-3 [Accessed: 26 August 2024]

انظر أيضاً:

Michael Veale and Frederik Zuiderveen, Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach, Computer Law Review International, vol. 22, no. 4, pp. 97–112, 2021, p. 106, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3896852 [Accessed: 26 August 2024]

[٣] انظر في ذلك:

Centre for Digital Governance, Op. cit.

وهو ما كان محلاً للنقد، لأن من شأن وضع الالتزام على المستخدمين أن يخلق فجوة قانونية يمكن استغلالها بسوء نية[١]. وأشار آخرون إلى أن المسؤولية عن استخدام أنظمة الذكاء الاصطناعي يجب أن تقع في المقام الأول على عاتق المزودين، وليس المُستخدمين[٢].

فقد عرفت المادة الثالثة "المُستخدم" بأنه شخص طبيعي أو اعتباري، أو سلطة عامة، أو وكالة، أو هيئة أخرى تستخدم نظام الذكاء الاصطناعي تحت سلطتها، باستثناء الحالات التي يتم فيها استخدامه في سياق نشاط شخصي غير مهني[٣]، في حين أن "المزود" هو شخص طبيعي أو اعتباري، أو سلطة عامة، أو وكالة، أو هيئة أخرى تقوم بتطوير نظام ذكاء اصطناعي أو نموذج ذكاء اصطناعي للأغراض العامة[٤]، أو قامت بتطويره وطرحه في السوق أو

---

[١] انظر في ذلك:
Francesca Palmiotto, Detecting Deep Fake Evidence with Artificial Intelligence A Critical Look from a Criminal Law Perspective, 2023, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4384122 [Accessed: 26 August 2024]

[٢] انظر في ذلك:
Natali Helberger and Nicholas Diakopoulos, ChatGPT and the AI Act, Internet Policy Review, vol. 12, no. 1, 2023, pp. 3-5, available at: https://policyreview.info/essay/chatgpt-and-ai-act [Accessed: 26 August 2024]

[٣] انظر في ذلك: الفقرة ٤ من المادة الثالثة من قانون الذكاء الاصطناعي الصادر من الاتحاد الأوروبي والتي تنص على:
"Deployer" means a natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity."

[٤] تشير أنظمة الذكاء الاصطناعي ذات الأغراض العامة إلى الأنظمة التي تتمتع بمجموعة واسعة من الاستخدامات المحتملة، ويمكن تطبيقها على العديد من المهام في مجالات مختلفة. وقد أصبحت هذه الأنظمة ذات فائدة تجارية متزايدة نظرًا لتوفر كميات متزايدة من الموارد

وضعه في الخدمة تحت اسمها أو علامتها التجارية، سواء كان ذلك مقابل أجر أو مجانًا[١]. وبالتالي، فإن الالتزام بالشفافية يطبق فقط على مستخدمي تقنية التزييف العميق دون مزودي الخدمة، طالما أن فعل التزييف العميق لم يصل إلى فئة الأنظمة عالية الخطورة كما تناولنا سابقًا.

ويرتبط الالتزام بالشفافية بالالتزام بالتمييز المنصوص عليه في الفقرة الثانية من المادة ٥٠ بأنه "يجب على مُقدِمي أنظمة الذكاء الاصطناعي، بما في ذلك أنظمة الذكاء الاصطناعي للأغراض العامة، التي تولد محتوى صوتيًا أو صورة أو فيديو أو نصيًا اصطناعيًا، ضمان تمييز مخرجات نظام الذكاء الاصطناعي بتنسيق قابل للقراءة آليًا واكتشافها على أنها تم إنشاؤها أو معالجتها بشكل مصطنع...."[٢].

المالية للمطورين، بالإضافة إلى الأساليب المبتكرة لاستخدامها. وتتميز بقدرتها على تحقيق أغراض متعددة، سواء كانت مقصودة أو غير مقصودة من المطورين، وكذلك بإمكانياتها الكبيرة في تخزين الذاكرة والبيانات. وتشمل التطبيقات المحتملة لهذه الأنظمة التعرف على الصور والكلام، وإنشاء الصوت والفيديو، واكتشاف الأنماط، والإجابة على الأسئلة، والترجمة، وغيرها. انظر في ذلك:

Future of Life, General Purpose AI and the AI Act, May 2022, pp. 3-4, available at: https://shorturl.at/DbMoC [Accessed: 14 Septmber 2024]

[١] انظر في ذلك:

Paragraph 3 of Article 3 of the EU AI Act. It provides that "provider" means a natural or legal person, public authority, agency or other body that develops an AI system or a general-purpose AI model or that has an AI system or a general-purpose AI model developed and places it on the market or puts the AI system into service under its own name or trademark, whether for payment or free of charge."

[٢] انظر في ذلك:

Article 50/2 of the EU AI Act.

وأمام عدم التوضيح الدقيق لكيفية تحقيق هذه الالتزامات، يجب على اللوائح والقرارات التي تصدر من المفوضية لتنفيذ هذا القانون، أن تأخذ في الاعتبار هذه النقاط فيما يتعلق بمكافحة التزييف العميق وتطبيق التزامات الشفافية والتمييز، وذلك تنفيذاً للمادة ٩٦ من القانون التي نصت على أن "تضع المفوضية المبادئ التوجيهية بشأن التنفيذ العملي لهذه اللائحة، وخاصة فيما يتعلق بما يلي: ... (د)التنفيذ العملي لالتزامات الشفافية المنصوص عليها في المادة ٥٠..."[١].

وقررت المادة ٤/٩٩ من القانون عقوبة عدم الامتثال للالتزامات المتعلقة بالشفافية والتي قد تخضع لغرامات إدارية تصل إلى ١٥ مليون يورو أو، إذا كان الجاني مؤسسة، تصل إلى ٣٪ من إجمالي مبيعاتها السنوية على مستوى العالم للسنة المالية السابقة، أيهما أعلى[٢].

[١] المادة ٩٦ من قانون الذكاء الاصطناعي الصادر من الاتحاد الأوروبي.

[٢] المادة ٤/٩٩ من قانون الذكاء الاصطناعي الصادر من الاتحاد الأوروبي.

الخاتمة

يفرض التزييف العميق تحدياً هائلاً على الاستخدامات والأنشطة في العالم الافتراضي الذي أصبح المجال الأكثر أهمية في العصر الحالي. فأصبح مؤخراً أحد أهم تقنيات الذكاء الاصطناعي التي أثارت جدلاً واسعاً حول استخداماتها وأهمية التنظيم القانوني لها.

وقد تعرضنا لهذه الظاهرة في هذا البحث، وقد توصلنا إلى مجموعة من النتائج والتي من أهمها:

النتائج:

أولاً: يمكن تعريف التزييف العميق بأنه صورة أو محتوى صوتي أو فيديو تم إنشاؤه أو التلاعب به بواسطة الذكاء الاصطناعي بهدف مماثلة أشخاص، أو أشياء، أو أماكن، أو كيانات، أو أحداث معينة، ويظهر – على غير الحقيقة– للشخص العادي أنه أصلي أو صحيح.

ثانياً: قد يكون للتزييف العميق فوائد عديدة مثل الانتاجات الرسومية الصوتية، والاستخدامات الطبية والبحثية، وفي مؤتمرات الفيديو. كما أنه قد يكون له أضرار نفسية ومالية، وأضرار مجتمعية تؤثر على العملية الديمقراطية والعدالة الجنائية، وأضرار ماسة بالأمن القومي والعلاقات الدولية.

ثالثاً: يتميز التزييف العميق بمجموعة من الخصائص أهمها الطبيعة التقنية كأحد تقنيات الذكاء الاصطناعي، والطبيعة النمطية المتعلقة بالمحتوى الذي يقع عليه فعل التزييف (صورة أو فيديو، أو مقطع صوتي)، والنتيجة الخاصة المتمثلة في انتاج المحتوى المزيف، وخداع المتلقيين، والأثر المترتب على هذا الخداع.

رابعاً: يمكن اعتبار فعل التزييف العميق فعلاً محظوراً بموجب المادة ٥ من قانون الذكاء الاصطناعي، وذلك في الحالة التي يستخدم فيها بشكل مُتعمَد للتأثير في تشويه سلوك شخص أو مجموعة من الأشخاص بشكل ملموس، بما يؤدي ذلك إلى إضعاف قدرتهم على اتخاذ قرار مستنير بشكل ملحوظ، مما يدفعهم إلى اتخاذ قرار لم يكونوا ليتخذوه لولا ذلك.

خامساً: يمكن اعتبار فعل التزييف العميق ضمن الفئات عالية الخطورة وفقاً للمادة ٦ من القانون وذلك بأن يكون في أحد القطاعات الثمانية التي تضمنها الملحق الثالث من القانون. وذلك فيما عدا: المهام الإجرائية الضيقة، وتحسين نتائج الأنشطة البشرية المكتملة سابقًا، واكتشاف أنماط اتخاذ القرار دون التأثير على النتائج، والمهام التحضيرية للتقييمات.

سادساً: تُطبَق التزامات الشفافية والتمييز على أفعال التزييف العميق كقاعدة عامة، وذلك فيما عدا أنظمة الذكاء الاصطناعي المُصرَح بها لأغراض إنفاذ القانون، وفي الأعمال الفنية أو الإبداعية التي لا تعيق الشفافية الاستمتاع بها.

سابعاً: تُطبَق عقوبات على مخالفة الالتزامات المنصوص عليها في القانون بالنسبة لكل فئة، والتي قد تصل إلى غرامات قيمتها ٣٥ مليون يورو، أو نسبة من إجمالي المبيعات، وذلك فقاً لكل حالة على حده.

كما توصلنا من خلال هذه الدراسة إلى مجموعة من التوصيات أهمها:

أولاً: الحاجة إلى شمول تعريف التزييف العميق لأي محتوى مزيف، ليشمل النصوص الكتابية على سبيل المثال، وألا يكون مقصوراً فقط على الصور

والفيديوهات ومقاطع الصوت. وذلك بهدف إضفاء أكبر قدر من الحماية ضد التزييف العميق.

ثانياً: الحاجة إلى النص على التزييف العميق بنصوص صريحة في كل فئة من الفئات لحسم الجدال بشأنها، كما فعل بالنسبة للالتزام بالشفافية الوارد في المادة ٥٠ من القانون. وبذلك يجب على المفوضية أن تراعي ذلك في المبادئ التوجيهية التي ستصدرها بشأن التنفيذ العملي لهذه القانون.

ثالثاً: الحاجة إلى قواعد أكثر ردعاً فيما يتعلق بمخالفة أحكام القانون، لصعوبة تنفيذ بعض الالتزامات على الدول والجهات الفاعلة من غير الدول. وبذلك قد يصبح نطاق تطبيق القانون محدود على الشركات والأفراد العاديين، وهو ما يغفل الحماية من التزييف العميق ضد هذه الجهات.

رابعاً: الحاجة إلى قواعد تفصيلية خاصة بكيفية تصنيف فعل التزييف العميق إلى فئة معينة من الفئات الواردة في القانون. وكذلك الحاجة إلى قواعد خاصة بتنفيذ التزامات الشفافية والتمييز المنصوص عليها في القانون.

خامساً: يجب أن تولي المنظمات الأخرى، مثل جامعة الدول العربية والاتحاد الأفريقي، اهتماماً بمواجهة أنظمة الذكاء الاصطناعي وتنظيمها بصورة جيدة، حيث إن المواجهة الداخلية وحدها غير مجدية عند الحديث عن هذه التقنيات. وبالتالي، تحتاج إلى تضافر الجهود الدولية لمواجهة ذلك.

سادساً: الحاجة إلى تبادل المعرفة والخبرات من خلال مشاركة المعلومات حول أفضل الممارسات في استخدام الذكاء الاصطناعي لتعزيز قدرة الدول والمنظمات الدولية في مواجهة التحديات. كما يجب تطوير استراتيجيات مشتركة لمواجهة المخاطر المرتبطة بالذكاء الاصطناعي، مثل الخصوصية

والأمان. بالإضافة إلى ذلك، يُعتبر تعزيز التعليم والتوعية هدفاً مهماً لزيادة الوعي حول الذكاء الاصطناعي وتأثيراته على المجتمع والمستقبل.

قائمة المراجع

أولاً: المراجع باللغة العربية:

١ – الكتب:

- أبو الخير عطيه، قانون التنظيم الدولي، مطبعة الفجيرة الوطنية، دبي، طبعة ٢٠٠٧.
- أحمد أبو الوفا، الوسيط في القانون الدولي العام، دار النهضة العربية، طبعة ٢٠٠٤.
- أحمد محمد البوشي، الابتزاز الإلكتروني مفهوم جديد في جرائم التهديد المعلوماتية: دراسة تفصيلية في ضوء قانون العقوبات وقانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ وأحدث أحكام محكمة النقض المصرية، دار النهضة العربية، ٢٠٢٢.
- حسين عبد الكريم، خليل يوسف الجندي، الابتزاز الإلكتروني والجرائم الإلكترونية – المفهوم والأسباب، دار كفاءة المعرفة للنشر والتوزيع، عمان، ٢٠١٩.
- خالد ممدوح إبراهيم، التنظيم القانون للذكاء الاصطناعي، دار الفكر الجامعي، الإسكندرية، ٢٠٢٢،.
- صلاح الدين عامر، مقدمة لدراسة القانون الدولي العام، طبعة ٢٠٠٢، دار النهضة العربية.
- محمد طلعت الغنيمي، الوسيط في القانون الدولي العام، الدار الجامعية، طبعة ٢٠٠٣.

- هلالي عبد اللاه أحمد، الجوانب الموضوعية والإجرائية لجرائم المعلوماتية، دار النهضة العربية، ٢٠٠٦.

٢ – الأبحاث:

- أحمد محمد الخولى، المسئولية المدنية الناتجة عن الاستخدام غير المشروع لتطبيقات الذكاء الاصطناعي "الديب فيك نموذجاً"، مجلة البحوث الفقهية والقانونية العدد ٣٦، أكتوبر ٢٠٢١.

- أحمد مصطفى معوض، استخدامات الذّكاء الاصطناعي استخدام تقنية التزيِيف العميق في قذف الغير نموذجًا دراسة فقهية مقارنة معاصرة، مجلة البحوث الفقهية والقانونية، العدد ٣٩، أكتوبر ٢٠٢٢.

- اسلام دسوقي عبد النبي، دور تقنيات الذكاء الاصطناعي في العلاقات الدولية والمسئولية الدولية عن استخداماتها، المجلة القانونية، ٢٠٢٠.

- أشرف سيد أبو العلا، المواجهة الجنائية لتقنية الديب فيك، مجلة العلوم القانونية والاقتصادية، يناير ٢٠٢٤.

- حسام محمد السيد محمد، المواجهة الجنائية لظاهرة الثأر الإباحي دراسة مقارنة بين النظامين الأنجلو أمريكي واللاتيني الجزء الثاني، مجلة الدراسات القانونية والاقتصادية، المجلد ٥ العدد ٢، ديسمبر، ٢٠١٩.

- عمرو طه بدوي محمد، النظام القانوني للروبوتات الذكية المزودة بتقنية الذكاء الاصطناعي (الإمارات العربية المتحدة كنموذج) دراسة تحليلية مقارنة لقواعد القانون المدني للروبوتات الصادرة عن الاتحاد الأوروبي سنة ٢٠١٧ ومشروع ميثاق أخلاقيات الروبوت الكوري، مجلة الدراسات القانونية والاقتصادية،٢٠٢١.

- أ.د/ محمد صافي يوسف، تدبير حماية الأمن القومي كاستثناء على تطبيق قواعد القانون الدولي العام، المجلة المصرية للقانون الدولي، ٢٠١٠.
- محمد مشعل، الذكاء الاصطناعي وآثاره علي حرية التعبير في مواقع التواصل الاجتماعي، مجلة البحوث القانونية والاقتصادية، كلية الحقوق جامعة المنصورة، المجلد ١١، العدد ٧٧، سبتمبر، ٢٠٢١.
- يحي إبراهيم دهشان، المسئولية الجنائية عن جرائم الذكاء الاصطناعي، مجلة الشريعة والقانون، جامعة الإمارات، ٢٠١٩.

٣- التقارير:

- تقرير الهيئة السعودية للبيانات والذكاء الاصطناعي، مبادئ أخلاقيات الذكاء الاصطناعي، أغسطس ٢٠٢٢.
- دليل التزييف العميق، البرنامج الوطني للذكاء الاصطناعي، الإمارات العربية المتحدة، يوليو ٢٠٢١.

ثانياً: المراجع باللغة الإنجليزية:

١- الأبحاث والدوريات:

- Adrienne de Ruiter, The Distinct Wrong of Deepfakes, Philosophy & Technology, vol. 34, 2021, available at: https://link.springer.com/article/10.1007/s13347-021-00459-2 [Accessed: 14 August 2024].

- Andy Ramos et al, The first Artificial Intelligence Act is here. Key aspects, June 2024, available at: https://www.perezllorca.com/wp-content/uploads/2024/06/05-TechLaw-IA_La-primera-regulacion-de-la-Inteligencia-Artificial-ya-esta-aqui.-Aspectos-clave_ENG.pdf [Accessed: 27 July 2024].

- Angelica Fernandez, "Deep fakes": disentangling terms in the proposed EU Artificial Intelligence Act, UFITA Archiv für Medienrecht und Medienwissenschaft, vol. 85, no. 2, pp. 392–433, 2021, available at: https://shorturl.at/vSEdL (Accessed: 1 September 2024).

- B. van der Sloot, Y. Wagensveld, "Deepfakes: regulatory challenges for the synthetic society," Computer Law & Security Review, vol. 46, 2022, available at: https://www.sciencedirect.com/science/article/pii/S0267364922000632?ref=pdf_download&fr=RR-2&rr=8b5e4ddfdb230fe6 [Accessed: 10 August 2024].

- Bart van der Sloot et al, Deepfakes: The Legal Challenges of the Synthetic Society, Tilburg Institute for Law, Technology, and Society, 2021, available at: https://shorturl.at/Hz38W [Accessed: 15 August 2024].

- Bo Zhao et al., Deep fake geography? When geospatial data encounter Artificial Intelligence, Cartography and Geographic Information Science, vol. 48, no. 4, pp. 338–352, 2021, available at: https://www.tandfonline.com/doi/full/10.1080/15230406.2021.1910075 [Accessed: 1 September 2024].

- Casey Becker and Robin Laycock , Embracing deepfakes and AI-generated images in neuroscience research, European Journal of Neuroscience, vol. 58, no. 3, 2023, available at:

https://onlinelibrary.wiley.com/doi/10.1111/ejn.16052 [Accessed: 14 August 2024].

- Catherine Kerner and Mathias Risse, 'Beyond Porn and Discreditation: Epistemic Promises and Perils of Deepfake Technology in Digital Lifeworlds,' Moral Philosophy and Politics, November 11, 2020, available at: https://doi.org/10.1515/mopp-2020-0024 [Accessed: 29 July 2024].

- Centre for Digital Governance, The false promise of transparent deep fakes: How transparency obligations in the draft AI Act fail to deal with the threat of disinformation and image-based sexual abuse, Hertie School, 2022. Available at: https://rb.gy/m0nm7c [Accessed: 21 August 2024]

- CHRISTOPHER KLEIN, How Germany's Invasion of Poland Kicked Off WWII, History, 2014, available at: https://www.history.com/news/world-war-ii-begins-german-invasion-poland-1939 [Accessed: 29 July 2024]

- Cristian Vaccari and Andrew Chadwick, Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News, Social Media + Society, vol. 6, no. 1, 2020, available at: https://journals.sagepub.com/doi/10.1177/2056305120903408 [Accessed: 15 August 2024].

- Cristina Mesa, Deep fakes: the media and the legal system is under threat, 2023, available at: https://shorturl.at/171b4 [Accessed: 22 August 2024].

- Danielle K. Citron and Robert Chesney, Deep Fakes: A Looming Challenge for Priv es: A Looming Challenge for Privacy, Democr , Democracy, and National Security, California Law Review, 2019, available at: https://scholarship.law.bu.edu/faculty_scholarship/640 [Accessed: 29 July 2024].

- Danielle K. Citron and Robert Chesney, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," California Law Review, vol. 107, no. 18, pp. 1753–1820, 2019, p. 1767, available at: https://shorturl.at/Q1Ygg [Accessed: 26 August 2024]

- David J. Oberly, Analyzing the EU Artificial Intelligence Act: Spotlight on Biometrics, Baker Doneslon, 16 May 2024, available at: https://shorturl.at/N3n6k [Accessed: 18 August 2024]

- E. Pashentsev, "The Malicious Use of Deepfakes Against Psychological Security and Political Stability," in The Palgrave Handbook of Malicious Use of AI and Psychological Security, E. Pashentsev, Ed. London: Palgrave Macmillan, Cham, 2023, available at: https://journals.indexcopernicus.com/search/article?articleId=3752854 [Accessed: 27 July 2024].

- European Commission, 'New Rules for Artificial Intelligence – Questions and Answers,' Text, 2021, available at: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683

- Europol, Facing reality? Law enforcement and the challenge of deepfakes, an observatory report from the Europol Innovation Lab, Publications Office of the European Union, 2022, available at: https://shorturl.at/fBe72 [Accessed: 15 August 2024].

- EY, The European Union Artificial Intelligence Act, 12 July 2024, available at: https://www.ey.com/content/dam/ey-unified-site/ey-com/en-gl/insights/public-policy/documents/ey-gl-eu-ai-act-07-2024.pdf [Accessed: 25 July 2024].

- 'Facebook Is Building the Future of Connection with Lifelike Avatars,' Facebook Technology, March 13, 2019, available at: https://tech.facebook.com/reality-labs/2019/3/codec-avatars-facebook-reality-labs/ [Accessed: 29 July 2024].

- Federal Trade Commission, Combatting Online Harms Through Innovation, Federal Trade Commission Report to Congress, 2022, available at: https://shorturl.at/R8k2n [Accessed: 13 August 2024].

- Felix Juefei-Xu et al., Countering Malicious DeepFakes: Survey, Battleground, and Horizon, International Journal of Computer Vision, vol. 130, no. 7, 2022, available at: https://arxiv.org/pdf/2103.00218 [Accessed: 27 July 2024].

- Francesca Palmiotto, Detecting Deep Fake Evidence with Artificial Intelligence A Critical Look from a Criminal Law Perspective, 2023, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4384122 [Accessed: 26 August 2024]

- Future of Life, General Purpose AI and the AI Act, May 2022, pp. 3-4, available at: https://shorturl.at/DbMoC [Accessed: 14 September 2024]

- Greg Allen and Taniel Chan, Artificial Intelligence and National Security, Cambridge: Belfer Center for Science and International Affairs, July 2017, available at: https://www.belfercenter.org/publication/artificial-intelligence-and-national-security [Accessed: 29 July 2024]

- Henry Farrell, Abraham Newman, and Jeremy Wallace, "Spirals of Delusion," Foreign Affairs, September/October 2022, available at: https://www.foreignaffairs.com/world/spirals-delusion-artificial-intelligence-decision-making [Accessed: 29 July 2024]

- How to tell reality from a deepfake?, World Economic Forum, April 2021, available at: https://www.weforum.org/agenda/2021/04/are-we-at-a-tipping-point-on-the-use-of-deepfakes/ [Accessed: 29 July 2024]

- James Pearson and Natalia Zinets, "Deepfake Footage Purports to Show Ukrainian President Capitulating," Reuters, 17 March 2022, available at: https://www.reuters.com/world/europe/deepfake-footage-purports-show-ukrainian-president-capitulating-2022-03-16/ [Accessed: 29 July 2024]

- Jason Lyall, Divided Armies: Inequality and Battlefield Performance in Modern War, Princeton University Press, 2020, available at: https://academic.oup.com/ia/article/97/2/573/6159415 [Accessed: 29 July 2024]

- John R. Allen and Darrell M. West, The Brookings glossary of AI and emerging technologies Commentary, The Brookings, 13 July 2020, available at: https://www.brookings.edu/articles/the-brookings-glossary-of-ai-and-emerging-technologies/ [Accessed: 10 August 2024].

- Jon Bateman, Deepfakes and Synthetic Media in the Financial System: Assessing Threat Scenarios, Carnegie Endowment for International Peace, July 2020, p. 22, available at: https://shorturl.at/IlgU0 [Accessed: 29 July 2024].

- Josh A. Goldstein et al., Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations, 2023, available at: https://arxiv.org/abs/2301.04246 [Accessed: 13 August 2024]

- Joshua Habgood-Coote, Deepfakes and the epistemic apocalypse, Synthese, vol. 201, no. 3, 2023, available at: https://link.springer.com/article/10.1007/s11229-023-04097-3 [Accessed: 26 August 2024]

- K. Giles, K. Hartmann, M. Mustaffa, The Role of Deepfakes in Malign Influence Campaigns. Riga: NATO Strategic Communications Centre of Excellence, 2019, available at: https://stratcomcoe.org/pdfjs/?file=/publications/download/web_deep_fakes_report_11-08-2019.pdf?zoom=page-fit [Accessed: 10 August 2024].

- Latham & Watkins, EU AI Act: Navigating a Brave New World, July 2024, available at : https://www.lw.com/en/admin/upload/SiteAttachments/EU-AI-Act-Navigating-a-Brave-New-World.pdf [Accessed: 27 July 2024].

- Lilian Edwards, Regulating AI in Europe: four problems and four solutions, Ada Lovelace Institute, 2022, available at: https://shorturl.at/qCgfY [Accessed: 14 August 2024],

- Lilian Edwards, The EU AI Act proposal. Ada Lovelace Institute, 2022, available at: https://www.adalovelaceinstitute.org/wp-content/uploads/2022/04/Expert-explainer-The-EU-AI-Act-11-April-2022.pdf [Accessed: 25 July 2024].

- Luke Hurst, How a fake image of a Pentagon explosion shared on Twitter caused a real dip on Wall Street, 2023, available at: https://www.euronews.com/next/2023/05/23/fake-news-about-an-explosion-at-the-pentagon-spreads-on-verified-accounts-on-twitter [Accessed: 1 September 2024].

- Maria Pawelec, Deepfakes and Democracy (Theory): How Synthetic Audio-Visual Media for Disinformation and Hate Speech Threaten Core Democratic Functions, Digital Society, vol. 2, no. 2, 2022, available at: https://doi.org/10.1007/s44206-022-00010-6 [Accessed: 25 July 2024].

- Mateusz Łabuz, Regulating Deep Fakes in the Artificial Intelligence Act, ACIG, vol. 2, no. 1, 2023, available at: https://shorturl.at/dJWxh [Accessed: 20 August 2024]

- Matthew N. O. Sadiku, DATA MINING: A BRIEF INTRODUCTION, European Scientific Journal, vol.11, No.21, July

2015, available at: https://core.ac.uk/download/pdf/328025049.pdf [Accessed: 29 July 2024].

- Matúš Mesarčík et al., Stance on The Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence – Artificial Intelligence Act, Kempelen Institute of Intelligent Technologies, 2021, available at: https://zenodo.org/doi/10.5281/zenodo.12567879 [Accessed: 21 August 2024]

- Michael Veale and Frederik Zuiderveen, Demystifying the Draft EU Artificial Intelligence Act — Analysing the good, the bad, and the unclear elements of the proposed approach, Computer Law Review International, vol. 22, no. 4, pp. 97–112, 2021, available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3896852 [Accessed: 26 August 2024].

- Min Liu and Xijin Zhang, Deepfake Technology and Current Legal Status of It, Proceedings of the 2022 3rd International Conference on Artificial Intelligence and Education (IC-ICAIE 2022), 27 December 2022, available at: https://www.atlantis-press.com/proceedings/ic-icaie-22/125981029 [Accessed: 25 July 2024].

- Mohaiminul Islam et al, An Overview of Neural Network, American Journal of Neural Networks and Applications, 5(1): 7-11, 2019, available at: http://www.sciencepublishinggroup.com/j/ajnna [Accessed in: 25 July 2024].

- Natali Helberger and Nicholas Diakopoulos, ChatGPT and the AI Act, Internet Policy Review, vol. 12, no. 1, 2023, available at: https://policyreview.info/essay/chatgpt-and-ai-act [Accessed: 26 August 2024]

- Prativa Barik, An Overview of AI Techniques and Their Applications, Journal of Nonlinear Analysis and Optimization Vol. 11, Issue. 1, 2020, available at: https://www.jnao-nu.com/Vol_11_Issue_01_January-June_2020/62.pdf [Accessed: 29 July 2024].

- R. Mattioli, A. Malatras, Identifying Emerging Cyber Security Threats and Challenges for 2030. Athens: ENISA, 2023, p. available athttps://shorturl.at/Ne7aU [Accessed: 10 August 2024].

- R. T. Toparlak, "Criminalising Pornographic Deep Fakes: A Gender-Specific Inspection of Image-Based Sexual Abuse," SciencesPo Law School The 10th Graduate Conference, 2022,

Available: https://www.sciencespo.fr/public/chaire-numerique/wp-content/uploads/2022/06/3a-Toparlak_Criminalising-Pornographic-Deep-Fakes.pdf [Accessed in: 29 July 2024].

- Ranjan Mishra et al, The Understanding of Deep Learning: A Comprehensive Review, Mathematical Problems in Engineering, 5 April 2021, p. 1, available at: https://onlinelibrary.wiley.com/doi/10.1155/2021/5548884 [Accessed: 29 July 2024].

- Regina Rini, Deepfakes and the Epistemic Backstop, Philosopher's Imprint 20, no. 24, 2020, available at: https://philpapers.org/archive/RINDAT.pdf [Accessed: 29 July 2024].

- Robert Chesney and Danielle Citron, "Deepfakes: A Looming Crisis for National Security, Democracy and Privacy?", Lawfare, 2018, available at: https://www.lawfaremedia.org/article/deepfakes-looming-crisis-national-security-democracy-and-privacy [Accessed: 29 July 2024]

- Ruchi Bisht, What is Deepfake AI?, InfosecTrain, November 2023, available at: https://www.infosectrain.com/blog/what-is-deepfake-ai/

- Rüya Tuna Toparlak, "Criminalising Pornographic Deep Fakes: A Gender-Specific Inspection of Image-Based Sexual Abuse," SciencesPo Law School The 10th Graduate Conference, 2022, available at: https://rb.gy/mnsnpn [Accessed: 21 August 2024]

- Sarah Cahlan, 'How Misinformation Helped Spark an Attempted Coup in Gabon, Washington Post, 2020, available at: https://shorturl.at/05j9k [Accessed: 29 July 2024].

- Sathesh Sriskandarajah, Computer Vision Fundamentals for Business Leaders PricewaterhouseCoopers, April 2020, p. 5, available at: https://www.pwc.com.au/consulting/assets/pwc-computer-vision-fundamentals-for-business-leaders.pdf [Accessed: 29 July 2024].

- Snapshot Paper - Deepfakes and Audiovisual Disinformation, Independent report, 12 September 2019, available at: https://shorturl.at/gQvUV [Accessed: 29 July 2024].

- Steve Blank, Artificial Intelligence/ Machine Learning Explained, Gordian Knot Center for National Security Innovation, 12 May 2022, available at: https://gordianknot.stanford.edu/publications/artificial-intelligence-machine-learning-explained (Accessed: 29 July 2024)

- Tackling deepfakes in European policy, EPRS | European Parliamentary Research Service, July 2021, available at: https://shorturl.at/gSZRw [Accessed: 29 July 2024].

- Thomas Rid, Active Measures: The Secret History of Disinformation and Political Warfare, Volume 64, No. 1, March 2020, available at: https://shorturl.at/YzdK8 [Accessed: 29 July 2024]

- Tom Dobber et al., 'Do (Microtargeted) Deepfakes Have Real Effects on Political Attitudes?,' The International Journal of Press/Politics, July 25, 2020, available at: https://journals.sagepub.com/doi/10.1177/1940161220944364 [Accessed: 29 July 2024].

- Tom Simonite, "A Zelensky Deepfake Was Quickly Defeated. The Next One Might Not Be," WIRED, March 17, 2022, available at: https://www.wired.com/story/zelensky-deepfake-facebook-twitter-playbook/ [Accessed: 29 July 2024]

- Tor Constantino, Is AI quietly killing itself – and the Internet?, Forbes, 2024, available at: https://shorturl.at/e6nKM [Accessed: 29 July 2024]

- Vincenzo Ciancaglini et al., Malicious Uses and Abuses of Artificial Intelligence, Trend Micro Research, 2020, available at: https://documents.trendmicro.com/assets/white_papers/wp-malicious-uses-and-abuses-of-artificial-intelligence.pdf [Accessed: 29 July 2024].

- W Lance Bennett and Steven Livingston, 'The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions,' European Journal of Communication 33, no. 2, 1 April 2018, 122–39, available at: https://journals.sagepub.com/doi/10.1177/0267323118760317 [Accessed: 29 July 2024].

- Ziolkowski and others v Land Berlin, Case C-424/10 and C-425/10, EU:C:2011:866, 2011, available at: https://eu.vlex.com/vid/judgment-of-the-court-838702989

٢- التقارير والقوانين والأحكام:

- ANNEX III High-risk AI systems referred to in Article 6(2), REGULATION (EU) 2024/1689 OF THE EUROPEAN

PARLIAMENT AND OF THE COUNCIL No. 2024/1689 ,13 June 2024.

- Bundesrat (Federal Council), Resolution of the Federal Council. Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legal acts, 2021, available: Microsoft Word - Vorblatt 210468-0 (bundesrat.de) [Accessed: 22 August 2024]

- Case C-803/79 Gérard Roudolff EU:C:1980:166, para 7, available at: https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX%3A61979CJ0803

- European Commission, Proposal for Regulation of the European Parliament and the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts. COM (2021) 206 final. 2021, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206

- European Commission, Proposal for Regulation of the European Parliament and the Council laying down harmonized rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain union legislative acts. COM (2021) 206 final. 2021, available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206 [Accessed: 26 August 2024]

- European Parliament, Amendments adopted by the European Parliament on 14 June 2023 on the proposal for a regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts. (COM 2021)0206 – C9-0146/2021 – 2021/0106(COD))1. P9_TA (2023)0236. 2023. Available at: https://www.europarl.europa.eu/doceo/document/TA-9-2023-0236_EN.html [Accessed: 20 August 2024].

- European Parliament›s Committee on Legal Affairs, Report on artificial intelligence: questions of interpretation and application of international law in so far as the EU is affected in the areas of civil and military uses and of state authority outside the scope of criminal justice. 2020/2013(INI). 2021, available at:

https://www.europarl.europa.eu/doceo/document/A-9-2021-0001_EN.html [Accessed: 26 August 2024]

- INFORMATION FROM EUROPEAN UNION INSTITUTIONS, BODIES, OFFICES AND AGENCIES, EUROPEAN COMMISSION, COMMISSION NOTICE The 'Blue Guide' on the implementation of EU product rules 2022, (2022/C 247/01), 29 June 2022, para. 5, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022XC0629(04)

- Proposal for a Directive on combating violence against women and domestic violence, COM/2022/105 final, 2022.

- REGULATION (EU) 2024/1689 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 June 2024, No. 2024/1689, Official Journal of the European Union, 12 July 2024, available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj [Accessed: 25 July 2024].

- The Digital Services Act package, The European Commission, 25 July 2024, available at: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package [Accessed: 1 September 2024].

- The European Commission, High-Level Expert Group on Artificial Intelligence, ETHICS GUIDELINES FOR TRUSTWORTHY AI, 8 April 2019, available at: https://www.aepd.es/sites/default/files/2019-12/ai-ethics-guidelines.pdf [Accessed: 27 August 2024]

- Ziolkowski and others v Land Berlin, Case C-424/10 and C-425/10, EU:C:2011:866, 2011, available at: https://eu.vlex.com/vid/judgment-of-the-court-838702989