

## جرائم الذكاء الاصطناعي وسبل مواجهتها: جرائم التزييف العميق نموذجًا

علاء الدين منصور مغايرة

أستاذ القانون الجنائي المساعد، كلية القانون، جامعة عجمان-الإمارات العربية المتحدة

a.maghaireh@ajman.ac.ae

### ملخص

تأتي هذه الدراسة في ظل تطور متسارع لتطبيقات الذكاء الاصطناعي وشيوع استعمالها على نطاق واسع من قبل مختلف فئات المجتمع؛ حيث تهدف الدراسة إلى تسليط الضوء على ظاهرة جديدة ومستحدثة من جرائم الذكاء الاصطناعي يطلق عليها اسم تقنية التزييف العميق (Deepfake) والتي تعد من بين الموضوعات الحديثة في مجال العلم الجنائي لم تنل بعد اهتمام الباحثين بالقدر الكافي في ميادين علم القانون الجنائي، فهناك عدد قليل من الدراسات العربية والغربية التي تناولت جرائم تقنية التزييف العميق دون التوسع في تبيان أنواعها وسبل المواجهة، وتتمثل مشكلة البحث في الكشف عن طبيعة الجرائم التي يمكن أن ترتكب باستخدام تطبيقات التزييف العميق وبيان مدى كفاءة النصوص القانونية الحديثة الخاصة بالتزييف العميق للحد من ظاهرة الاستخدام الخبيث لهذه التقنية، وقد اعتمد الباحث على المنهج الاستقرائي التحليلي والمنهج الوصفي المعتمد على جمع المعلومات من مختلف المصادر الأكاديمية وغير الأكاديمية، إضافة إلى الاستعانة بالمنهج المقارن. وقد انتهى البحث إلى عدة نتائج، من أهمها: أن تقنية التزييف العميق سلاح ذو حدين إيجابي مفيد وسلب ضار يمكن استخدامها لارتكاب العديد من الجرائم التقليدية بأسلوب حديث. ولذلك أوصينا بضرورة إصدار تشريع خاص بالتزييف العميق يتناول أنواع الجرائم وعقوبة كل منها، وقيمة التعويض عن الأضرار التي تترتب على كل جريمة. وبالتالي تسهم الدراسة في إثراء المعرفة القانونية والأكاديمية حول هذه التقنية وتأثيراتها، وتوفير إطار قانوني للتعامل مع المخاطر المرتبطة بها، وتقديم نموذج للدراسات المستقبلية في هذا المجال.

**الكلمات المفتاحية:** التزييف العميق، تعريف التزييف العميق، مشروعية التزييف العميق، جرائم التزييف

العميق، قانون التزييف العميق، مواجهة التزييف العميق

للاقتباس: مغايرة، علاء الدين منصور. «جرائم الذكاء الاصطناعي وسبل مواجهتها: جرائم التزييف العميق نموذجًا»، المجلة الدولية

للقانون، جامعة قطر، المجلد الثالث عشر، العدد المنتظم الثاني، 2024. <https://doi.org/10.29117/irl.2024.0301>

© 2024، مغايرة، الجهة المرخص لها: دار نشر جامعة قطر. تم نشر هذه المقالة البحثية وفقاً لشرط Creative Commons Attribution-Non-

Commercial 4.0 International (CC BY-NC 4.0). تسمح هذه الرخصة بالاستخدام غير التجاري، وينبغي نسبة العمل إلى صاحبه، مع

بيان أي تعديلات عليه. كما تتيح حرية نسخ، وتوزيع، ونقل العمل بأي شكل من الأشكال، أو بأية وسيلة، ومزجه وتحويله والبناء عليه، طالما

يُنسب العمل الأصلي إلى المؤلف. <https://creativecommons.org/licenses/by-nc/4.0>

## Artificial Intelligence Crimes and Countermeasures: Deepfake Crimes as a Model

**Alaeldin Mansour Maghaireh**

Assistant Professor of Criminal Law, Law College, Ajman University-UAE  
a.maghaireh@ajman.ac.ae

### Abstract

The rapid development of artificial intelligence applications and their widespread use has triggered this study. It aims to shed light on an emerging phenomenon of artificial intelligence crimes, known as Deepfake technology. This topic is among the modern subjects in the field of criminology that has not yet received sufficient attention. There are few Arab and Western studies that have addressed Deepfake technology without elaborating on its types and countermeasures. The research problem centers around the nature of the crimes that can be committed using Deepfake applications and examining the extent to which Anti-Deepfake laws are effective against malicious use of this technology. The researcher adopted an inductive analytical approach and a descriptive method based on gathering information from various academic and non-academic sources. Additionally, a comparative approach was used. The research concluded with several results, the most important of which are: Deepfake technology is a double-edged sword that can be used to commit traditional crimes in a modern way. Therefore, we recommended the need to issue special legislation for Deepfake that addresses the types of crimes, punishment and compensation for the damages resulting from each crime. Thus, the study contributes to enriching legal and academic knowledge about this technology and its effects, providing a legal framework for dealing with the risks associated with it, and offering a model for future studies in this field.

**Keywords:** Deepfake definition; Legitimacy of Deepfake; Deepfake crimes; Deepfake laws; Deepfake countermeasure

**Cite this article as:** Maghaireh A.M. "Artificial Intelligence Crimes and Countermeasures: Deepfake Crimes as a Model" *International Review of Law*, Qatar University, Volume 13, Regular Issue 2, 2024. <https://doi.org/10.29117/irl.2024.0301>

© 2024, Maghaireh A.M., licensee, IRL & QU Press. This article is published under the terms of the Creative Commons Attribution Non-Commercial 4.0 International (CC BY-NC 4.0), which permits non-commercial use of the material, appropriate credit, and indication if changes in the material were made. You can copy and redistribute the material in any medium or format as well as remix, transform, and build upon the material, provided the original work is properly cited. <https://creativecommons.org/licenses/by-nc/4.0>

## مقدمة

يشهد العالم تطورًا متسارعًا لتطبيقات الذكاء الاصطناعي وشيوع استعمالها على نطاق واسع من قبل مختلف فئات المجتمع؛ حيث أصبحت جزءًا أساسيًا في تطبيقات مواقع التواصل الاجتماعي، فقبل عقدين من الزمن كانت قدرة الأفراد على إنتاج وتوزيع المحتوى الرقمي محدودة للغاية؛ حيث كانت تسيطر الحكومات وبعض المؤسسات الإعلامية العالمية على المحتوى الإعلامي، سواء على المستوى الوطني أو العالمي، وفي مقابل ذلك كان دور الأفراد يقتصر على استقبال المحتوى دون القدرة على إنتاجه أو إعادة تدويره حتى وصول الإنترنت ومن ثم العديد من التطبيقات الاجتماعية ومواقع التواصل الاجتماعي التي جعلت الأفراد قادرين على إنتاج المحتوى الإعلامي، وحتى التلاعب بمحتواه المرئي والصوتي، وبالرغم من ذلك ما زالت الوسائط الرقمية الحديثة من تسجيلات مرئية وصوتية محل ثقة لدى الكثير من المستخدمين حيث يشير المحتوى المتداول بالصوت والصورة إلى صاحبه بشكل قاطع، وليس هناك شك في أن ذلك المحتوى المرئي أو الصوتي لا يعكس الحقيقة والواقع. لكن يؤكد أن الحقيقة والواقع في خطر مع وصول أحد تطبيقات الذكاء الاصطناعي (Artificial Intelligence)، ويسمى تطبيق التزييف العميق (Deepfake)، ولهذا التطبيق جانب إيجابي يتمثل في عدد من الاستخدامات المفيدة مثل الإبداع والترفيه والتعليم والإعلام وغيرها من المجالات، وفي المقابل هناك الجانب المظلم، فهذا التطبيق الذكي قد يسقط بيد ضعاف النفوس والمجرمين ليستخدم كأداة فعالة في ارتكاب العديد من الجرائم يطلق عليها اسم «جرائم التزييف العميق» (Deepfake Crimes). وقد أشار الخبراء في هذا المجال إلى حتمية انتشار وشيوع تقنية التزييف العميق في المستقبل القريب لعدة أسباب من أهمها سهولة إنتاج المحتوى<sup>1</sup> دون الحاجة إلى مهارات تقنية<sup>2</sup>، ويقابل ذلك صعوبة كشف حقيقتها<sup>3</sup>، أو استحالة ذلك مع التطور والتحديث المستمر للذكاء الاصطناعي<sup>4</sup>.

## مشكلة الدراسة

تتمثل مشكلة البحث في ظهور وتطور نمط جديد من تقنيات الذكاء الاصطناعي يطلق عليه اسم التزييف العميق وقد تترتب على الاستخدام السيء لهذه التقنية أضرار جسيمة بالأفراد والمؤسسات الخاصة والعامة، ولا شك في أن تعدد تقنيات الذكاء الاصطناعي وشيوع استخدامها يثير العديد من المشكلات، وي طرح العديد من التساؤلات الأخلاقية والقانونية، ولكننا في هذا البحث نتساءل عن طبيعة الجرائم التي يمكن أن ترتكب باستخدام

1 T. Brooks, et, al, Increasing Threat of Deepfake Identities. Homeland Security, USA. Department of Homeland Security, [https://www.dhs.gov/sites/default/files/publications/increasing\\_threats\\_of\\_deepfake\\_identities\\_0.pdf](https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf). (last visited June 5, 2023).

2 B. Chesney & D. Citron, Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, California Law Review, (107) (2019) 1753.

3 V. Petkauskas, Report: Number of Expert-Crafted Video Deepfakes Double Every Six Months, (September 28, 2021). <https://cybernews.com/privacy/report-number-of-expert-crafted-video-deepfakes-double-every-six-months>, (last visited 09/07/2023).

4 J. Burt, Deepfakes being used in 'sextortion' scams, FBI warns (2023). [https://www.theregister.com/2023/06/08/ai\\_deepfakes\\_sextortion\\_fbi](https://www.theregister.com/2023/06/08/ai_deepfakes_sextortion_fbi). (last visited June 9, 2023); H. Dixon, Deepfakes: More Frightening Than Photoshop on Steroids, Judges Journal, Vol. 58, N. 3 (2019) 36.

تطبيقات التزييف العميق ومدى كفاءة النصوص القانونية الحديثة الخاصة بالتزييف العميق مقابل قصور القوانين التقليدية أو السيرانية للحد من ظاهرة الاستخدام الخبيث لهذه التقنية، لذا ستحاول هذه الدراسة أن تجيب عن عدة تساؤلات أبرزها يكمن في ما يلي: ماهية تقنية التزييف العميق؟ ومدى مشروعية هذه التقنية؟ وما هي الجرائم التي يمكن أن ترتكب باستخدامها؟ وماهي سبل المواجهة للحد من الاستخدام الخبيث لهذه التقنية؟

## أهداف الدراسة

تهدف هذه الدراسة إلى تسليط الضوء على ظاهرة جديدة ومستحدثة من جرائم الذكاء الاصطناعي يطلق عليها «التزييف العميق» (Deepfake) وذلك بعرض الجوانب الهامة التي تحيط بتلك التقنية، وبيان فوائدها وأضرارها وعرض الجرائم التي ارتكبت والجرائم التي يحتمل ارتكابها والآثار الناتجة عن سوء الاستخدام، وتحليل بعض الجوانب القانونية الرئيسية المتعلقة بها لمعرفة ما إذا كان استخدام هذه التقنية بحد ذاته يشكل جريمة، وبالتالي من الواجب النص عليها صراحة في نصوص قانون الجرائم الإلكترونية، أم أن القوانين الحالية سواء التقليدية أو السيرانية قادرة على مواجهة الاستخدام السيئ لهذه التقنية وبالتالي لا حاجة لتدخل تشريعي، فهذه التقنية وما تشكله من خطر على حياة الأفراد والسلم في المجتمع واستقرار الدولة تتطلب دراسة هذا النوع من سوء استخدام الذكاء الاصطناعي، ودراسة تجارب الدول التي سارعت في إصدار التشريعات الحديثة لمواجهة، وبالنتيجة المساهمة في إثراء الدراسات العربية القانونية حول هذه الظاهرة المستحدثة.

## أهمية الدراسة

تكمن أهمية اختيار الموضوع في كون الظواهر الإجرامية المستحدثة، كظاهرة التزييف العميق والتي تعد من صور جرائم الذكاء الاصطناعي تعد من بين الموضوعات الحديثة جداً في مجال العلم الجنائي والتي لم تنل بعد اهتمام الباحثين الجنائيين بالقدر الكافي في ميادين علم القانون الجنائي، فهناك عدد قليل من الدراسات العربية والغربية التي تناولت بعض جرائم تقنية التزييف العميق دون التوسع إلى تبيان أنواعها، وذلك على الرغم من آثارها الخطيرة التي يمكن أن تنتج عنها وتمس الأفراد والمؤسسات العامة والخاصة، ومن هنا كان ضرورياً الوقوف على الدراسات والتجارب الغربية والتي سبقت مثيلاتها العربية حول هذه الجرائم الحديثة.

## منهجية الدراسة

نظراً لأهمية المسائل التي يعالجها هذا الموضوع وارتباطها بتقنيات الذكاء الاصطناعي وخصوصاً تقنية التزييف العميق، فإنه يتطلب من الباحث عرض تفاصيل تتعلق بكيفية عمل هذه التقنية، والفوائد التي يمكن استخدامها لها ثم عرض مخاطرها من خلال طرح عدد من السيناريوهات لمعرفة حجم المشكلة التي قد تنجم عن استخدامها، والأخطار الناجمة عنها، وحيث إنها ظاهرة مستحدثة لم تنل الاهتمام الأكاديمي بشكل كافي، وبالتالي ندرة المراجع الأكاديمية الأجنبية والعربية التي تتناول هذا الموضوع، لذا سوف نعتمد على عدد كبير من التقارير الحكومية

5 T.J. Hancock & N.J. Bailenson, The Social Impact of Deepfakes, Cyberpsychology, Behaviour, and Social Networking, Vol. 24, No. 3 (2021) 149.

والمواقع الإلكترونية بمختلف أنواعها والمراجع الأجنبية التي تتناول تقنية التزييف العميق، لذلك سنعتمد في هذا البحث على المنهج الاستقرائي التحليلي والمنهج الوصفي المعتمد على جمع المعلومات والحقائق من مختلف المصادر الأكاديمية وغير الأكاديمية. إضافةً إلى الاستعانة بالمنهج المقارن ببعض الدول المتقدمة في تطوير تشريعاتها.

## خطة الدراسة

إن متطلبات الدراسة العلمية وطبيعة الموضوع والغرض من بحثه تجعل من المناسب أن نعالج هذا الموضوع من خلال مقدمة، ومطلب تمهيدي، ومبحثين وخاتمة؛ حيث نتناول في المطلب التمهيدي: مفهوم التزييف العميق، وفي المبحث الأول أشكال ومفهوم جرائم التزييف العميق، أما المبحث الثاني؛ فيتناول سبل مواجهة جرائم التزييف العميق.

## مطلب تمهيدي: مفهوم التزييف العميق

يشهد العصر الحالي تطورًا متسارعًا في مجال تطبيقات الذكاء الاصطناعي، مما أدى إلى ظهور تحديات جديدة ومستجدة في العالم الرقمي وأحد أهم هذه التحديات هو انتشار ظاهرة «التزييف العميق»، وهي ظاهرة تقنية تستند إلى الاستفادة من تطور التقنيات الحديثة لإنشاء محتوى معدل بشكل يصعب التفريق بينه وبين المحتوى الأصلي، وليبان هذه الظاهرة ومعرفة أسرارها سيتم تقسيم هذا المطلب إلى فرعين: تعريف التزييف العميق ومشروعيته.

## الفرع الأول: تعريف التزييف العميق

للإحاطة بمفهوم التزييف العميق لا بد من معرفة كيفية وطبيعة عمل التزييف العميق.

### أولاً: كيفية عمل التزييف العميق

التزييف العميق هو نتاج أحد تطبيقات تقنيات الذكاء الاصطناعي يسمى نموذج التعليم العميق (Deep Model Learning) ومن هذا الاسم يمكن التعرف على أهم خصائص هذا النموذج وهو التعليم التلقائي أو الذاتي، وهو متخصص بإنشاء صور ومقاطع فيديو مرئية وصوتية (voice cloning or synthetic voice) للشخص المستهدف طبق الأصل من نسخته الأصلية، وبالتالي القدرة على إنتاج نسخة مزيفة طبق الأصل ذات محتوى مختلف تمامًا عن الحقيقة، بحيث تبدو واقعية إلى حد التطابق بين النسختين الأصلية والمزيفة، فنكون أمام فيديو لذات الشخص المستهدف صوتًا وصورة لكن بحركات وتصرفات وبيئة محيطة به لا تمثل حقيقة الواقع لذلك الشخص<sup>6</sup>. وبالنتيجة يكون لها تأثير يتخطى كل أشكال التزييف التقليدية وغير التقليدية المعروفة كالصورة العادية المفبركة أو الأخبار المكتوبة.

هذا يتم بشكل رئيسي عن طريق استخدام شبكات ذكية وعصبية عميقة تسمى «شبكات التوليد المعارض» (Generative Adversarial Networks) التي اخترعت من قبل الباحث في شركة جوجل إيان قودفلو (Ian

6 T. Dobber, et al., Do (Microtargeted) Deepfake Have Real Effects on Political Attitudes? The International Journal of Press/Politics, Vol. 26 (1) (2021), p. 72.

(Goodfellow) عام 2014 وهي عبارة عن شبكتين متضادتين تتعلمان من بعضهما البعض من خلال التنافس بينهما، فالشبكة الأولى تسمى المميز (Discriminator) والثانية تسمى المولد (Generator)؛ حيث تقوم الشبكة الأولى بالكشف أو التمييز بين البيانات المزيفة والحقيقية للمحتوى بينما تسعى الشبكة الثانية إلى إنشاء بيانات أكثر إقناعاً للواقع بحيث لا يمكن للشبكة الأولى المميز تمييزها عن البيانات الحقيقية<sup>7</sup>، وتستمر هذه العملية التنافسية بين الشبكتين حتى تتمكن الشبكة الثانية من خلق محتوى يصعب تمييزه عن الحقيقة من قبل الشبكة الأولى المميز<sup>8</sup>. ولتوضيح ذلك لتتخيل شخصاً ما يريد أن ينتج صورة غير حقيقية لصورة الموناليزا من خلال استخدامه لعدد من الصور الحقيقية لها حيث يقوم المولد بإنشاء صورة لها غير دقيقة ومشوشة فيقوم المميز وبشكل سريع بالكشف عن أنها غير حقيقية بالمقارنة مع الصورة الحقيقية، مما يدفع ذلك المولد إلى التعلم وبالتالي إنتاج صورة أخرى مختلفة عن الأولى وبإعادة تلك الحلقات من الكشف والتعلم حتى ينتج المولد صورة أفضل وأقرب إلى الحقيقة والواقع مقابل عجز المميز عن التمييز بينها وبين الصورة الحقيقية<sup>9</sup>. وهذا المثال ينطبق على الصور المتحركة والسمعية، كذلك يمكن تشبيه النموذج التوليدي بفريق من الموزعين يحاولون تزوير عملة نقدية واستخدامها دون كشف في حين يكون النموذج التمييزي مشابهاً للشرطة التي تحاول الكشف عن العملة المزورة حيث تشتغل المنافسة بين الفريقين المزيف والشرطي حتى يصعب التمييز بين العملات الاصلية والمزيفة<sup>10</sup>.

في بدايات ظهور تقنية التزييف العميق كان المستخدم يحتاج إلى تحليل مجموعة كبيرة من المحتوى الرقمي والبيانات المتعلقة بالشخص المستهدف لتوليد ملامح واقعية جديدة للوجه أو الصوت أو كليهما، لكن مع التطور الهائل والمستمر لهذه التقنية أصبح بالإمكان إنتاج المحتوى المزيف باستخدام الهاتف المحمول من خلال تطبيق (Reface)<sup>11</sup> أو غيره من تطبيقات أصبحت منتشرة وفي متناول الجميع؛ حيث وصل عددها حتى وقت إعداد هذا البحث إلى خمسة عشر تطبيقاً<sup>12</sup>، وبالتالي يمكن من خلال استخدام صورة واحدة ودون الحاجة إلى خبرة في ذلك<sup>13</sup>، أو من خلال حصول المستخدم على تسجيل صوتي قصير للشخص المستهدف أن يتمكن من إنتاج الفيديو المزيف<sup>14</sup>.

7 Chesney & Citron, supra note 2, p. 1760.

8 L. Daniel et al., Deepfakes and International Conflict, The Brookings Institution, Washington DC. (2023), p. 3.

9 Ibid.

10 I.J. Goodfellow et al., Generative Adversarial Nets. NeurIPS. [https://proceedings.neurips.cc/paper\\_files/paper/2014/file/5ca3e9b122f61f8f06494c97b1afccf3-Paper.pdf](https://proceedings.neurips.cc/paper_files/paper/2014/file/5ca3e9b122f61f8f06494c97b1afccf3-Paper.pdf) (last visited June 5, 2023).

11 G. Fowler, Anyone with an iPhone Can Now Make Deepfakes. We Aren't Ready for What Happens Next (2021), The Washington Post. <https://www.washingtonpost.com/technology/2021/03/25/deepfake-video-apps/>. (last visited Jun 01, 2023).

12 Shivangi, A, 15 Best Deepfake Apps & Websites that You Must Try (2023). <https://www.smartprix.com/bytes/14-best-deepfake-apps-websites-for-entertainment/>. (last visited Aug 09, 2023).

13 Fowler, supra note 11; R. Tolosana, et al., An Introduction to Digital Face Manipulation, In Handbook of Digital Face Manipulation and Detection: From DeepFakes to Morphing Attacks, Christian Rathgeb, et al (eds.) Springer, 2022. 4.

14 A. Rehan, «12 AI Voice Cloning Tools to Create Seamless Authentic Voiceovers,» (2023). <https://geekflare.com/ai-voice-cloning-tools/?s=12+AI+Voice+Cloning+Tools+to+Create+Seamless+Authentic+Voiceovers>. (las visited Aug 09, 2023).

## ثانيًا: تعريف التزييف العميق

الوصول إلى تعريف جامع مانع لظاهرة التزييف العميق لن يوقف تطورها وانتشارها؛ حيث يشير معظم الباحثين إلى شيوع استخدامها بشكل سيء وعلى نطاق واسع في المستقبل القريب، وبالتالي الوصول إلى تعريف واضح وشامل، بقدر الإمكان، سوف يساعد على فهم هذه الظاهرة والوصول إلى حلول قانونية قد تمنع هذا الانتشار<sup>15</sup>. يتكون التزييف العميق من مصطلحين الأول العميق "deep" والمصطلح الثاني التزييف "fake"، فالأول يشير إلى نوع برامج الذكاء المستخدمة - نموذج التعليم العميق (Learning Deep Model) - أما المصطلح الثاني فهو يعني تزييف الحقيقة والواقع، ويشير بعض الخبراء إلى أن هذا المصطلح «التزييف العميق» يدل على الاستخدام غير الشرعي لتقنية التعليم العميق<sup>16</sup>. وحتى هذه اللحظة ليس هناك تعريف أو مصطلح يميز بين الاستخدام الإيجابي والاستخدام السلبي لهذه التقنية، ونحن نؤكد هنا وندعو إلى وجوب استخدام مصطلح مختلف للتمييز بين «التزييف العميق الإيجابي»، و«التزييف العميق السلبي» بحيث يشير الأول إلى الاستخدام الأخلاقي لهذه التقنية، على أن يشير الثاني إلى الاستخدام غير الأخلاقي وإحداث الضرر للآخرين. لقد عرف تقرير برلمان الاتحاد الأوروبي التزييف العميق بأنه «عبارة عن وسائل صوتية، أو بصرية معدلة، أو مصنعة تبدو حقيقية، وتصور شخصًا أو أشخاصًا يظهرهم وكأنهم يقولون أو يفعلون شيئًا لم يقولوه أو يفعلوه أبدًا، ويتم إنتاجه باستخدام تكنولوجيا الذكاء الاصطناعي بما في ذلك التعلم الآلي والتعليم العميق»<sup>17</sup>. وعرفه البعض بأنه «الفيديو المنتج من خوارزميات التعلم العميق (Deep Algorithms Learning) من خلال برامج متاحة يسهل الوصول إليها وتمتع بالقدرة على إنتاج وتقديم محتوى محرف يخالف الحقيقة من خلال وضع وجه شخص مستهدف فوق جسد شخص آخر بدون تمييز على حدوث ذلك»<sup>18</sup>. وفي تعريف آخر أنه «تسجيلات صوتية أو مرئية تم تعديلها رقميًا باستخدام خوارزميات التعلم الآلي لخلق أحداث مزيفة لم تحدث أبدًا»<sup>19</sup>. ويعرف أليكس أنجلز التزييف العميق بأنه «عبارة عن مقاطع صوتية وصور وفيديوهات تظهر وكأنها حقيقية لكنها في الواقع اصطناعية تم إنشاؤها باستخدام تقنيات الذكاء الاصطناعي»<sup>20</sup>. يتضح من

15 J. Vincent, Why we Need a Better Definition of 'Deepfake.' (2018). <https://www.theverge.com/2018/5/22/17380306/deepfake-definition-ai-manipulation-fake-news> (last visited Jun 3, 2023)

16 K.A. Pantserev, The Malicious Use of AI-Based Deepfake Technology as the New Threat to Psychological Security and Political Stability. In: H. Jahankhani, et al. (ed.) Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity. Advanced Sciences and Technologies for Security Applications. Springer, Cham (2020). [https://doi.org/10.1007-3-978/3\\_7-35746-030](https://doi.org/10.1007-3-978/3_7-35746-030). (last visited Jun 5, 2023).

17 M. Huijstee et al., Tackling Deepfakes in European Policy. European Parliamentary Research Service (2021). [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS\\_STU\(2021\)690039\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf) (last visited Jun 14, 2023)

18 C. Chun Ki Chan, et al. Combating Deepfakes: Multi-LSTM and Blockchain as Proof of Authenticity for Digital Media (2020), IEEE/ITU <https://ieeexplore.ieee.org/abstract/document/9311067> (last visited July 17, 2023).

19 A. Barber, Freedom of Expression Meets Deepfakes. Synthese, 202(40) (2023). <https://doi.org/10.1007/s11229-023-4-04266>

20 A. Engler, Fighting deepfakes when detection fails. Brookings Institution (2019). <https://policycommons.net/artifacts/4139532/fighting-deepfakes-when-detection-fails/4947455>. CID: 20.500.12592/wvqgcb (last visited July 28, 2023).

عرض التعريفات أنها تركز على الخصائص التقنية وبالتالي نحتاج إلى تعريف قانوني يعكس طبيعة هذه التقنية ويميزها عن غيرها من تقنيات مشابهة. فهذه التقنية ذات حدين فقد تستخدم لأغراض حميدة أو لأغراض خبيثة، وبالتالي يمكننا تعريف التزييف العميق بأنه عبارة عن «أحد تطبيقات الذكاء الاصطناعي القادرة على إنشاء محتوى رقمي مرئي أو صوتي أو كليهما لشخص ما بشكل يحاكي الواقع ويخالف الحقيقة بغية الإضرار أو تحقيق مآرب أخرى».

### الفرع الثاني: مشروعية تقنية التزييف العميق

لقد ظهرت تقنية التزييف العميق في الأصل لأغراض التسلية<sup>21</sup> من قبل الأشخاص العاديين الذين يبحثون عن المتعة والتسلية والإثارة والإبداع، وتستخدم الآن على نطاق واسع في تطبيقات التواصل الاجتماعي مثل تيك توك، والكثير من التطبيقات المفيدة للبشرية، فهناك إنتاج محتوى كوميدي<sup>22</sup>، وربما هادف ولكن قد تترتب على ذلك عواقب وخيمة وأضرار تجاه الآخرين ويمكن توضيح ذلك من خلال أمثلة استخدام بعض مشاهير التواصل الاجتماعي وخصوصاً تطبيق تيك توك تقنية التزييف العميق لتصوير ضحايا جرائم القتل من خلال إعادة تمثيل الواقع بكافة الأحداث والشخصيات، وهذا يطرح الكثير من الأسئلة القانونية والأخلاقية حول هذا الاستخدام<sup>23</sup>. لكن سرعان ما تحولت إلى أداة بيد المجرمين، ويتوقع أن يفوق الاستخدام السلبي الاستخدام الإيجابي لها، مما أثار الجدل حول مشروعية صناعتها واستمرار تطويرها نظرًا للخطورة الكبيرة التي قد تنتج عن إساءة استخدامها. هناك جدل دائر بين رجال السياسة والقانون والتكنولوجيا حول مشروعية تقنية التزييف العميق بين من يعارض أو يؤيد وجودها، وبالتالي يمكن تقسيم ذلك إلى اتجاهين الأول يذهب إلى تأييد مشروعية وجود هذه التقنية، ويدعم حجته بالقول إن هذه التقنية كغيرها من أنواع أدوات التضليل المنتشرة في العالم الافتراضي وأن معظم الاستخدامات السيئة لها ينحصر في جرائم الإنتاج الإباحي<sup>24</sup>، ويدعو إلى عدم وضع قيود على استخدامها، ومن أشهر أصحاب هذا الرأي جيرانت ريس (Geraint Rees)<sup>25</sup>؛ حيث أكد الجانب الإيجابي والفوائد التي يمكن لهذه التقنية أن تقدمها للبشرية في عدة مجالات<sup>26</sup>، كذلك كيفن روز المحلل التكنولوجي في صحيفة نيويورك تايمز حيث ينقل عن مخترع تطبيق التزييف (FakeApp) قوله «لقد فكرت في الأمر ملياً وفي النهاية قررت أنه ليس من

21 M. Pic, et al., Face Manipulation Detection in Remote Operational System, in Handbook of Digital Face Manipulation and Detection: From DeepFakes to Morphing Attacks (Rathgeb et al. eds.), p. 431. (Springer 2022).

22 Á. Vizoso, M. Vaz-Álvarez & X. López-García, Fighting Deepfakes: Media and Internet Giants' Converging and Diverging Strategies Against Hi-Tech Misinformation, Media and Communication, 2021, Vol. 9, Issue 1, pp. 291–300 (2021). 293.

23 E. Dickson, AI Deepfakes of True-Crime Victims Are a Waking Nightmare (2023). <https://www.rollingstone.com/culture/culture-features/true-crime-tiktok-ai-deepfake-victims-children-1234743895/> (last visited Aug 22, 2023).

24 Ibid.

25 أستاذ علم الأعصاب المعرفي والذكاء الاصطناعي في جامعة كلية لندن في المملكة المتحدة. G. Rees, Here's how Deepfake Technology can Actually be a Good Thing, (2019) World Economic Forum, <https://www.weforum.org/agenda/11/2019/advantages-of-artificial-intelligenc/> /last visited August. (2023), 19

26 Ibid.

الصواب إدانة التكنولوجيا ذاتها والتي يمكن استخدامها في أغراض متعددة جيدة وسيئة<sup>27</sup>، وقد خالف كل من الباحثين ناثن كولانير ومايكل كوين ادعاء مخترع التقنية حيث قالوا إن الفوائد من استخدام هذه التقنية تتلاشى مقابل الأضرار المحتملة التي قد تسببها للمجتمع<sup>28</sup>، وهذا ما استند عليه أصحاب الاتجاه الثاني معارضين لهذه التقنية اعتمادًا على النتائج التي قد تترتب على الاستخدام السلبي من حيث قدرتها على التأثير على الرأي العام في المجتمع والإخلال بالحياة الديمقراطية وخصوصًا التلاعب بالرأي العام في الانتخابات<sup>29</sup> وإحداث زلازل سياسية أو اقتصادية أو اجتماعية مدمرة على نطاق واسع قد يصعب إصلاحها، وقد طالب البعض بحظر إنتاج أو تطوير مثل هذا النوع من الذكاء الاصطناعي الذي قد يترتب على استخدامه الكثير من الأضرار التي تفوق الفوائد من هذه التقنية، ونحن بدورنا نذهب مع الاتجاه الذي يدعم وجود هذه التقنية نظرًا إلى الاستخدامات الإيجابية التي يمكن تنفيذها باستخدام تقنية التزييف العميق في عدة مجالات كالصحة والإعلام والتعليم، لكن مع التشديد على ضرورة اتخاذ إجراءات قانونية وعملية تمنع من انتشار الاستخدام غير الأخلاقي وتعاقب على الاستخدام الضار.

### المبحث الأول: أشكال ومفهوم جرائم التزييف العميق

الجرائم التي يمكن أن ترتكب باستخدام تقنية التزييف العميق متعددة الأصناف والأشكال؛ حيث يمكن تقسيمها إلى نوعين من الجرائم، الأول يستهدف الأشخاص والثاني المجتمع والدولة، وبعد بحث تلك الجرائم في المطلب الأول نتناول المفهوم الطبيعي والاجتماعي للجريمة ومن ثم تطبيق تلك المفاهيم على جرائم التزييف العميق، ثم نتناول المفهوم القانوني للجريمة ومن ثم تطبيق الأركان العامة للجريمة على جرائم التزييف العميق وذلك في المطلب الثاني. وبالتالي يمكن تقسيم هذا المبحث إلى مطلبين في الأول نتناول الأشكال المختلفة لجرائم التزييف العميق وفي المطلب الثاني مفهوم الجريمة والتزييف العميق.

### المطلب الأول: أشكال جرائم التزييف العميق

يمكن لنا تقسيم جرائم التزييف العميق إلى طائفتين من الجرائم: الأولى تستهدف الأشخاص والمؤسسات الخاصة ونتناولها في الفرع الأول، وفي الفرع الثاني الجرائم التي تستهدف الدولة والمؤسسات العامة.

### الفرع الأول: جرائم التزييف العميق ضد الأشخاص والمؤسسات الخاصة

يعتمد التزييف العميق بالأساس على تغيير الحقيقة والواقع ويعتبر تغيير الحقائق والتلاعب بها قديماً قدم وجود الإنسان على هذه الأرض، لكن وبشكل لم يسبق له مثيل في تاريخ البشرية، تقدم هذه التقنية تصويراً يطابق الواقع بكل سهولة ويسر وبأقل تكلفة، وكل ذلك يجعلها أداة غير مسبوقه في يد المجرمين وضعاف النفوس لارتكاب

27 K. Roose, Here come the fake videos, too (2018). The New York Times. <https://www.nytimes.com/2018/03/04/technology/fake-videos-deepfakes.html> (last visited June 5, 2023)

28 N. Colaner & M.J. Quinn, Deepfakes and the Value-Neutrality Thesis (2020). <https://www.seattleu.edu/ethics-and-technology/viewpoints/deepfakes-and-the-value-neutrality-thesis.html> (last visited May 27, 2023).

29 J. Cook, Deepfake Technology: Assessing Security Risk. School of Informational Service (2022) AmericanUniversity. [https://www.american.edu/sis/centers/securitytechnology/deepfake\\_technology\\_assessing\\_security\\_risk.cfm](https://www.american.edu/sis/centers/securitytechnology/deepfake_technology_assessing_security_risk.cfm) (last visited August 19, 2023).

عدد كبير من الجرائم.

### أولاً: جرائم الابتزاز والانتقام الإباحي العميق

من الممكن توظيف هذه التقنية لتشويه سمعة الأفراد وإثارة النعرات الطائفية بين أفراد المجتمع وبث الفتنة ويمكن تخيل كثير من السيناريوهات لتحقيق مآرب شريرة تنال من شرف وسمعة الشرفاء وتخلق مشاكل اجتماعية تؤدي إلى زعزعة استقرار المجتمع وتطوره. كانت بدايات توظيف هذه التقنية مقتصرة على الانتقام الإباحي<sup>30</sup>، لكن شاع استخدامها فيما بعد لارتكاب جرائم متعددة ومختلفة بهدف الابتزاز وإثارة النعرات<sup>31</sup>.

يستخدم أصحاب النفوس المريضة وأصحاب النزعة الإجرامية تقنية التزييف العميق لتنفيذ مآربهم الإجرامية باستغلال ضعف الشخص المستهدف وخصوصاً الإناث، وتنفيذ الابتزاز للحصول على منافع مادية أو معنوية حيث من الممكن لمجرمي التزييف العميق استخدام هذه التقنية لابتزاز الشخص المستهدف مستغلاً ضعف القدرات التقنية، والإقناعية للضحية على كشف الحقيقة، وبدحض وتكذيب ما قد يصدر عن المزرور العميق من إنتاج فيديو يسيء للضحية، مما يدفعه للاستسلام لرغبات ومآرب المجرم تجنباً للأضرار التي قد تترتب على تنفيذ المجرم لتهديده بنشر الفيديو، ففي إحدى القضايا التي عرضت على القضاء الأمريكي عام 2010 ثبت قيام المدعو لويس ميجانجوس من ولاية ساننا آنا كاليفورنيا باختراق أجهزة كمبيوتر عدد من الضحايا الإناث حيث عثر المحققون في حوزته على 15000 تسجيل من كاميرات أجهزة الكمبيوتر و900 تسجيل صوتي و13000 لقطة خاصة بشاشات الضحايا البالغ عددهم 230 ضحية كان من ضمنهم 44 طفلاً وقد تمكن من الحصول على بعض الصور الخاصة بالضحايا ثم طلب الحصول على مقاطع فيديو إباحية للضحية مقابل عدم نشر صورها في مواقع التواصل الاجتماعي<sup>32</sup>، وبالنظر إلى هذه القضية وتطبيقها على تقنية التزييف العميق يستطيع المجرم إجبار الضحية على الخضوع لرغباته أو طلباته دون الحاجة إلى كل هذا الجهد والكمية من الصور والفيديوهات؛ حيث يستطيع من خلال استخدام صورة واحدة أو فيديو واحد إنتاج ذلك الفيديو.

كذلك تُستخدم التقنية لصناعة فيديوهات للانتقام من الشريك السابق، والمعروف أيضاً باسم الانتقام الإباحي، وهي من جرائم العنف الجنسي عبر الإنترنت<sup>33</sup>. ويقصد به «نشر صور عارية أو مقاطع فيديو جنسية لشخص ما، بشكل صريح على الإنترنت، عادة ما تتم عن طريق شريك جنسي سابق، دون موافقة الشخص المعني، ومن أجل التسبب في الضيق أو الحرج»<sup>34</sup>، وهي ليست من الجرائم المنتشرة أو التي تقع في المجتمعات العربية نظراً لعدد

30 Hancock & Bailenson, supra note 5, p. 150.

31 Vincent, supra note 15.

32 Benjamin Wittes et al., Sextortion: Cybersecurity, Teenagers, and Remote Sexual Assault (Brookings Institution, 2016). <https://www.brookings.edu/wp-content/uploads/2016/05/sextortion1-1.pdf> (last visited June 7, 2023).

33 S. Bothamley & Ruth, J. Tully, «Understanding Revenge Pornography: Public Perceptions of Revenge Pornography and Victim Blaming.» Journal of Aggression, Conflict and Peace Research (2018), doi: 10.1108/JACPR-09-2016-0253.

34 أحمد عبد الموجود زكير، «جريمة التزييف الإباحي العميق - دراسة مقارنة»، المجلة القانونية، جامعة القاهرة، كلية الحقوق (فرع الخرطوم)، مج 11، ع 7، 2022، ص 2233.

من الأسباب أهمها العادات والتقاليد التي تمنع حدوث علاقات خارج إطار الزواج، إلى جانب أهمية الشرف والعرض. وتعتبر جريمة الانتقام الإباحي من الجرائم السيبرانية التي عاجلها المشرع في الكثير من الدول الغربية، لكن مع ظهور تقنية التزييف العميق أصبح بمقدور الشريك استخدام صور الشريكة المنشورة والمتوفرة على مواقع التواصل الاجتماعي أو المواقع الإلكترونية، لتظهر بشكل مناف للحياء ثم استخدامها للانتقام من الشريك السابق<sup>35</sup>، وهي بذلك تشكل أكبر خطر على الشخص المستهدف وأكثر سهولة على المجرم، كذلك يعكف بعض صانعي التزييف العميق على عرض خدماتهم على مواقع التواصل الاجتماعي لقاء مبلغ من المال وصنع محتوى مزيف بناء على طلب الزبون بعد أن يقدم الأخير المعلومات الضرورية عن الشخص المستهدف بهدف الانتقام. كما يمكن تصوير شخصية سياسية أو إعلامية معروفة ومحاولة ابتزازها لتغيير موقفها أو التخلي عن المبادئ التي تؤمن بها، وبالتالي تصويرها أثناء القيام بأعمال وحركات لم تفعلها في واقع الأمر كما حدث للصحفية المعارضة للحركة القومية الهندية رنا أيوب عندما وقعت ضحية هذه التقنية من قبل أنصار اليمين المتطرف بتصويرها في مقطع فيديو إباحي تم نشره بشكل واسع على مواقع التواصل الاجتماعي في الهند<sup>36</sup>، وقد أدى ذلك إلى دخول الضحية إلى المستشفى لتعرضها إلى تسارع في ضربات القلب والقلق وارتفاع ضغط الدم<sup>37</sup>. إن تقنية التزييف العميق تفتح الكثير من الأبواب غير الأخلاقية وغير القانونية وغير الشرعية لكثير من المجرمين على مصراعها لارتكاب أشنع الجرائم في هذا المجال، وهو ما يستدعي تدخل المشرع بنصوص صريحة تحول دون انتشار هذه الأفعال وتعاقب الاستخدام السلبي لهذه التقنية وهو ما سنبحثه في المبحث الثاني.

### ثانيًا: جرائم الاحتيال العميق

الاحتيال من الجرائم التقليدية التي رافقت الثورة الصناعية ثم التكنولوجيا لتصبح من أكثر الجرائم شيوعًا في العصر الرقمي، وكما هو الحال مع دخول أدوات الاحتيال وطرائقه المختلفة إلى العالم الافتراضي سخر المجرمون تقنية التزييف العميق لخدمة أغراضهم الشريرة؛ حيث أصبح يستخدم على نطاق واسع في عمليات الاحتيال، فمثلاً قام عدد من المحتالين (Scammers) بتزوير شخصية رجل الأعمال الشهير إيلون ماسك بالترويج لنوع معين من العملات الرقمية حيث أظهره في الفيديو يقول «أنا هنا لأخبركم عن العملة الرقمية لنيورالينك (Neuralink crypto token) العملة الرقمية التي سوف تغير العالم إلى الأبد»<sup>38</sup>، مما دفع البعض إلى الاستثمار في تلك الأموال معتقدين أن الفيديو بالحقيقة يعود لرجل الأعمال إيلون ماسك<sup>39</sup>. وفي واقعة أخرى تعد الأولى من نوعها في استخدام

35 Burt, supra note 4.

36 K. Harrison & A. Leopold, et al., The State of Deepfake, Deeptrust Alliance (2020). <https://static1.squarespace.com/static/5d894b6dcd6a2255c38759fe/t/6046e099e1c70c281fe57447/1615257771315/Pornographic+Deepfake+Report+Part+1.pdf> (last visited July 11, 2023).

37 R. Ayyub, I Was the Victim of a Deepfake Porn Plot Intended to Silence Me, I Was The Victim Of a Deepfake Porn Plot Intended To Silence Me (2018). <http://huffingtonpost.co.uk> (last visited June 6, 2023).

38 M. Novak, Elon Musk Impersonator Scams Promise Free Neuralink Brain Chip in Paid Ads on Twitter (2023). <https://www.forbes.com/sites/digital-assets/202328/02//elon-musk-crypto-scams-promise-free-neuralink-brain-chip-in-paid-ads-on-twitter/?sh=75abe6d47b4f> (last visited June 7, 2023).

39 Ibid

تقنية التزييف العميق في الاحتيال، قام محتال سبيراني باستخدام صوت الرئيس التنفيذي لإحدى شركات الطاقة في ألمانيا وطريقة أسلوبه في الحديث بشكل تصعب معه معرفة حقيقة التزييف، ثم قام بالاتصال بالمدير العام لفرع الشركة في بريطانيا حتى اعتقد الأخير أنه على اتصال مع المدير العام في ألمانيا؛ حيث طلب منه القيام بتحويل مبلغ 243 ألف دولار إلى حساب بنكي لعميل في دولة هنغاريا<sup>40</sup>. وفي مايو 2023 وقع الممثل القانوني لشركة تكنولوجيا في الصين في عملية احتيال تم فيها استخدام تقنية التزييف العميق حيث قام بتحويل مبلغ مالي كبير إلى أحد أصدقائه بعد أن أجرى معه اتصالاً مرئياً ليتضح فيما بعد أنه كان مجرد ضحية للتزييف العميق<sup>41</sup>، كذلك تعتبر وسيلة سهلة للحصول على الأموال بطرق غير مشروعة من خلال استخدام إنتاج إعلانات تصور شخصيات ومشاهير يتحدثون عن تسويق منتجات دون موافقة أو علم هؤلاء الأشخاص، فمثلاً قامت شركة بتسويق أحد المنتجات يسمى (EcoChamp)<sup>42</sup> من خلال عمل فيديو بتقنية التزييف العميق يتحدث فيه أحد الخبراء في مجال الأمن السبيراني عن فعالية وفوائد الجهاز دون علمه أو موافقته على ذلك<sup>43</sup>، وقد اتضح أن المنتج ليس سوى عملية احتيال<sup>44</sup>. ومما لا شك فيه أن هذه الأمثلة ما هي إلا غيض من فيض ولكن المخفي أعظم فهناك الكثير من الجرائم التي تتم في الخفاء ولم يتم الإبلاغ عنها.

### ثالثاً: جرائم تشويه السمعة والانتقام

يتعرض الكثير من الناس إلى تشويه السمعة أو الانتقام عبر مواقع التواصل الاجتماعي والتطبيقات الحديثة من أشخاص معروفين للضحية أو مجهولي الهوية، كتوجيه عبارات الشتم والتحقير أو القذف أو عرض صور خاصة للضحية، لكن مع وصول تقنية التزييف العميق فالمخاطر والأضرار أصبحت أشد وطئاً، وربما من الصعوبة بمكان إصلاح الأضرار الناتجة عن استخدامها، وقد شكلت جرائم تشويه السمعة وخصوصاً المحتوى الإباحي المزييف ما نسبته 96٪ من استخدام التزييف العميق<sup>45</sup>، وحسب إحدى التقديرات الصادرة في شهر تشرين الأول من عام 2020 فقد بلغ عدد الصور الإباحية المزيفة 100 ألف صورة نشرت دون موافقة الضحية<sup>46</sup>، ومع انتشار

40 J. Damiani, A Voice Deepfake Was Used to Scam A CEO Out Of \$243,000 (2019). <http://forbes.com> (last visited June 7, 2023).

41 J. Zhang, AI-Deep Synthesis Regulations and Legal Challenges: Recent Face Swap Fraud Cases in China. Lexology. <https://www.lexology.com/library/detail.aspx?g=1a3455cc-dc4d-4ed0-918a-c3429999c31f>. (last visited August 24, 2023).

42 يدعي الإعلان أن المنتج الذي يطلق عليه اسم (EcoChamp) له القدرة على توفير الطاقة المنزلية، وهو عبارة عن احتيال لتسويق المنتج المذكور، لمزيد من المعلومات راجع:

B. Mariyam «Is Ecochamp a Scam? Review of Electricity Saving Device.» Online Threat Alerts (2022). <https://www.onlinethreatalerts.com/article/2022/9/10/is-ecochamp-a-scam-review-of-electricity-saving-device/> (last visited 26 May 2023).

43 V. Kropotov, et al. How Underground Groups Use Stolen Identities and Deepfakes (2022). [https://www.trendmicro.com/en\\_us/research/22/i/how-underground-groups-use-stolen-identities-and-deepfakes.html](https://www.trendmicro.com/en_us/research/22/i/how-underground-groups-use-stolen-identities-and-deepfakes.html) (last visited Aug 22, 2023).

44 Mariyam, supra note 42.

45 Petkauskas, supra note 3.

46 Brooks, et al., supra note 1, 17.

التقنية وسهولة استخدامها وانخفاض الكلفة<sup>47</sup> لا شك في تمديد المجرمين لتوظيفها السليبي في جميع مجالات الحياة سواء في بيئة العمل أو الدراسة أو النشاطات الرياضية، وفي دوائر العلاقات الاجتماعية والسياسية والاقتصادية وعالم الأعمال والمال، فهناك المتربصون من أصحاب النفوس الضعيفة التي تهدف إلى الإضرار بالآخرين سواء قصد أو غير قصد، وهذه التقنية تفتح لهم الأبواب أمام العديد من الفرص التي تمكنهم من تنفيذ مآربهم سواء من أجل الانتقام أو إبعاد الضحية عن المنافسة أو فرص النجاح في الوصول إلى أهدافه المشروعة، فقد أشارت إحدى الدراسات<sup>48</sup> إلى حجم الأضرار المترتبة على استخدامها، فقد تؤدي إلى ضياع وتدمير العلاقة بين الأزواج أو الإساءة إلى سمعة الشخص وابتعاد الناس عنه أو التعامل معه، وقد يفقد فرص الترقية في العمل أو المنافسة أو تضيع عليه فرص النجاح في العمل والأعمال، وغير ذلك من أضرار لا يمكن إصلاحها حتى بعد اكتشاف التزييف العميق، فمن السيناريوهات المطروحة، مثلاً خلال التحضيرات لمنافسة رياضية عالمية وقبل بدء المنافسة يتم نشر فيديو يصور أحد اللاعبين وهو يتعاطى المنشطات أو المواد المخدرة أو تصويره وهو يقوم بتقديم الهدايا الثمينة إلى لجنة الحكام مما يترتب عليه إبعاده عن المنافسة وضياع فرص الفوز، وبالتالي خسارة الملايين من الدولارات قبل معرفة حقيقة الفيديو المصور، وقد قامت سيدة أمريكية بإرسال فيديو وصور إلى مدرب فريق ابنتها ضمن فريق التشجيع يصور منافسة ابنتها وهي تحتسي الخمر وتدخن وهي عارية<sup>49</sup>. أو كأن يقوم أحد الأشخاص لمنع إتمام إجراءات الزواج أو تدمير العلاقة الزوجية بنشر فيديو يصور فيه أحد الطرفين أو الزوجين في وضع غير أخلاقي أو غير لائق، أو انخراطه في أعمال جنسية صريحة مما يترتب عليه تدمير تلك العلاقة وصعوبة ترميمها حتى بعد اكتشاف حقيقة الفيديو. فمثلاً تم على مواقع التواصل الاجتماعي والمواقع الإخبارية تداول تسجيل لأحد الفنانين العرب يتهجم فيه على الآخرين ويتلفظ بألفاظ بذيئة؛ حيث رد الفنان المستهدف خلال لقاء تلفزيوني بأن الفيديو مفبرك ومركب وقد تسبب له بأضرار بالغة، كذلك يمكن استخدامها لتشويه سمعة أحد المنتجات التجارية أو الصناعية بتصويره بما يخالف الحقيقة.

مما يزيد الأمور تعقيداً سهولة انتشار الفيديو المزور عبر وسائل التواصل الاجتماعي وصعوبة إزالته من الشبكة حيث يبقى متداولاً ومحفوظاً حتى بعد اكتشاف زيفه وستبقى أضراره الجسيمة باقية وهو ما يشكل ضرراً مستمراً على عكس تدمير السمعة عبر الكتابة وتوجيه عبارات الشتم أو القذف عبر وسائل التواصل الاجتماعي؛ حيث يزول الضرر بعد إزالة العبارات لكن يبقى الفيديو متداولاً، ويمكن العثور عليه عن طريق محركات البحث، وهذا الضرر قد يستمر فيما إذا أراد الضحية التقدم بطلب وظيفة في إحدى الشركات أو المؤسسات، ومن المعروف أن كثيراً من أصحاب العمل يجرون تدقيقاً حول المتقدمين للوظيفة باستخدام محركات البحث، وبالتالي سوف يظهر هذا الفيديو المزيّف أمام صاحب العمل الذي بلا شك سوف يرفض طلب توظيف الضحية<sup>50</sup>، فإحدى الدراسات

47 Ibid, 18; Engler, supra note 20.

48 M. Lenthang, Cheerleader's Mom Created Deepfake Videos to Allegedly Harass her Daughter's Rivals (2021). ABC News, <https://abcnews.go.com/US/cheerleaders-mom-created-deepfake-videos-allegedly-harass-daughters/story?id=7643759> (last visited 26 May, 2023); Dobber et al, supra note 6, p. 72.

49 Chesney & Citron, supra note 2, p. 1777; Fowler, supra note 11.

50 Chesney & Citron, supra note 2, p.1775.

التي أجريت عام 2018 أظهرت ما نسبته 70٪ من أرباب العمل يستخدمون محركات البحث للتحري حول المتقدمين للوظيفة، وبينت الدراسة أن ما نسبته 54٪ من المتقدمين للوظيفة قد تم رفض طلباتهم بناء على المعلومات الناتجة عن البحث عبر الإنترنت ومواقع التواصل الاجتماعي<sup>51</sup>.

#### رابعاً: جرائم التزييف العميق في التجسس وسرقة المعلومات الحساسة

ظهر نوع جديد من وسائل التجسس وسرقة المعلومات الحساسة باستخدام تقنية التزييف العميق، فبعد حصول المجرم على هوية أحد الضحايا أو بعد جمع معلومات كافيه عنه يقوم بالتقدم لوظيفة إلى شركة أو مؤسسة مالية فيقوم مكتب الموارد البشرية بالتواصل مع المجرم (المرشح للوظيفة) وتنظيم مقابلة معه عن بعد عبر الوسائل التقنية، فيقوم الضحية بعمل فيديو حي مزيف لصاحب الهوية بحيث يظهر أمام لجنة التوظيف وهو يتحدث ويحيب عن الأسئلة التي تطرح عليه بعد أن يكون قد استعد لذلك، وبعد حصوله على الوظيفة يستطيع الدخول إلى المعلومات السرية والبيانات التابعة للشركة أو المؤسسة التي وظفته، وقد ذكر مكتب التحقيقات الفيدرالية الأمريكي أن الغاية من ذلك هو الحصول على المعلومات السرية والتجسس<sup>52</sup>.

#### الفرع الثاني: جرائم التزييف العميق ضد الدولة والمؤسسات العامة

لا تقتصر جرائم التزييف العميق على إيذاء الأشخاص والمؤسسات الخاصة وإنما تشكل خطراً على المجتمع وعلى الدولة<sup>53</sup>، ولتوضيح ذلك سنعرض عدداً من السيناريوهات التي يمكن فيها استخدام تقنية التزييف العميق وقد استخدمت في بعض الحالات لارتكاب عدد من الجرائم ضد المجتمع أو الدولة.

#### أولاً: جرائم التزييف العميق ضد رجال الدولة والانتخابات

لقد استخدمت تقنية التزييف العميق لإنتاج فيديوهات وهمية تصور سياسيين بارزين وهم يقومون بأفعال غير قانونية أو غير أخلاقية أو يدلون بتصريحات كاذبة أو يقدمون معلومات غير صحيحة. وهي بذلك تقوض ثقة المواطنين بالدولة وتبعث صوراً سلبية لها مما ينتج عنه تشويه صورة الأحزاب التي ينتمي إليها الساسة أو مؤسسات الدولة المختلفة<sup>54</sup>، ومن الأمثلة البارزة على هذا النوع من التزييف تعرضت رئيسة مجلس النواب الأمريكي لاعتداء بأدوات التزييف العميق يظهرها بصورة غير أخلاقية كشخص مخمور وغير متزن وهي تدلي بحديث أمام الصحافة<sup>55</sup>.

51 R. Wong, Stop Screening Job Candidates' Social-Media (2021) Harvard Business Review, <https://hbr.org/2021/09/stop-screening-job-candidates-social-media> (last visited June 10, 2023).

52 E. Chickowski, Criminals Use Deepfake Videos to Interview for Remote Work. Dark Reading (2022). <https://www.darkreading.com/attacks-breaches/criminals-deepfake-video-interview-remote-work/> (last Visited August 22, 2023).

53 Hancock & Bailenson, supra note 5, p. 151.

54 Dobber, et al., supra note 6, p. 74.

55 حصد الفيديو أكثر من مليوني مشاهدة وقد رفض موقع التواصل الاجتماعي الفيسبوك (طلب إزالة المحتوى مدافعاً عن رفضه الطلب بحق حرية التعبير واقتصر الأمر على عدم عرضه للفيديو في مقدمة الأخبار. لمزيد من التفاصيل انظر:

L. Feiner, Facebook says the doctored Nancy Pelosi Video Used to Question her Mental State and Viewed Millions of Times Will Stay Up(2019) . <https://www.cnn.com/2019/05/24/fake-nancy-pelosi-video-remains-on-facebook-and-twitter.htm> (last visited March 7, 2023).

كذلك وقع الزعيمان الروسي والكوري ضحايا التزييف العميق حيث ظهر كل منهما في فيديو منفصل يتحدثان أمام التلفاز عن عدم الحاجة إلى التدخل في الانتخابات الأمريكية لكون انبهار الولايات المتحدة الأمريكية آتيا من الداخل وهو أمر وشيك<sup>56</sup>. يمكن أن تستخدم هذه الفيديوهات إلى جانب استخدام الذكاء الاصطناعي في إنشاء مواقع وهمية<sup>57</sup> لنشر أخبار زائفة وتضليل الجمهور وإضعاف النظام الديمقراطي، وكمثال على ذلك الفيديو الذي يصور رئيس الوزراء البريطاني الأسبق جونسون بوريس (Boris Johnson) وهو يؤيد معارضة زعيم حزب العمال جيرمي كوربن (Jeremy Corbyn) لمنصب رئيس الوزراء على التلفاز البريطاني<sup>58</sup>، كذلك الحال خلال الانتخابات الأمريكية الأخيرة 2020؛ حيث اتهمت الولايات المتحدة الأمريكية روسيا باستخدام تقنية التزييف العميق للإضرار بالنظام الديمقراطي والانتخابات في الولايات المتحدة<sup>59</sup>، إلى جانب التوقعات بشيوع استخدامها للتأثير على نتائج الانتخابات القادمة 2024<sup>60</sup>.

### ثانيًا: جرائم التزييف العميق ضد الصحافة والإعلام

أصبحت مواقع التواصل الاجتماعي ضمن المصادر الأساسية التي يلجأ إليها الأفراد للحصول على الأخبار بمختلف أنواعها، وبالتالي أصبحت الوسيلة الأولى التي يلجأ مجرمو التزييف العميق إلى استخدامها كأداة لبث ونشر المحتوى المزيف<sup>61</sup>؛ حيث أظهر عدد من الأبحاث التأثير السلبي الذي يمكن أن يحدثه استخدام تقنية التزييف العميق على المواقع الإخبارية، فقد أكدت إحدى الدراسات التي قام بها عدد من الباحثين في الهند أن التزييف العميق زعزع ثقة الجمهور بتلك المواقع<sup>62</sup>، وهي تشكل تحديا لدى الصحافة والصحفيين بالتمييز بين الأخبار الحقيقية والأخبار المزيفة وبالرغم من أن هذه المهمة لم تفارق الصحفيين منذ بداية الثورة الصناعية إلا أنها اليوم أمام تحد هو الأخطر<sup>63</sup>، وقد صرح مدير الأبحاث والتطوير في شركة الإعلام نيويورك تايمز أن أكبر تحد للصحافة

56 K. Hao & W.D. Heaven, The Year Deepfakes Went Mainstream. MIT Technology Review. (2020). <https://www.technologyreview.com/2020/12/24/1015380/best-ai-deepfakes-of-2020/> (last visited May 27, 2023).

57 Ellamey, M, Y., "Criminal Protection from disinformation during electoral campaigns in light of the legislative Criminal Policy – A Comparative Study with Egyptian and French Legislations" (in Arabic) *International Review of Law*, Volume 9, Issue 3, 2020 Special Issue on the conference of "Law and Media: Horizons and Challenges"

58 A. Bienkov, Boris Johnson Appeared to Endorse Jeremy Corbyn for Prime Minister in a Convincing Deepfake Video (2019). <https://www.businessinsider.com/video-boris-johnson-endorses-jeremy-corbyn-in-convincing-deepfake-2019-11> (last visited July 14, 2023).

59 Chesney & Citron, supra note 2, p. 1777.

60 A. Ulmer & Anna Tong. Deepfaking it: America's 2024 Election Collides with AI Boom, (2023) <https://www.reuters.com/world/us/deepfaking-it-americas-2024-election-collides-with-ai-boom-2023-05-30/> (last visited July 14, 2023).

61 Vizoso, Vaz-Álvarez and López-García, supra note 22, p. 292.

62 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*, 6(1).

63 K. Wahl-Jorgensen & M. Carlson, Conjecturing Fearful Futures: Journalistic Discourses on Deepfakes. *Journalism Practice*, 15(6), 803–820 (2021).

وللمشاهدين اليوم يتمثل في قدرة المشاهد على تمييز الأخبار الموثوقة على الإنترنت<sup>64</sup>، فمثلاً وقوع الطالبة الأمريكية (إما غونزاليس) الناجية من المجزرة التي حدثت في ولاية فلوريدا عام 2018 ضحية التزييف العميق حيث شاركت الطالبة في مسيرة في مدينة واشنطن ضد اقتناء الأسلحة، وقد ظهرت في صورة وهي تمزق لوحة تمثل رمز اقتناء الأسلحة، لكن تم استبدالها بتقنية التزييف العميق بلوحة تمثل الدستور الأمريكي<sup>65</sup>، فهذا الفيديو يشكل تحدياً للصحافة والصحفيين من جهة والمشاهد من جهة أخرى. فالأول يجد أن دوره أصبح يقتصر على التمييز بين الخبر الحقيقي والخبر المزيف وهذا يستنزف الوقت والجهد أما المشاهد فيفقد الثقة في الإعلام.

### ثالثاً: جرائم التزييف العميق ضد نظام القضاء والعدالة

مع ظهور وشيوع استخدام تقنية التزييف العميق سوف يتشكل لدى الجمهور الشك حول مصداقية الأدلة المرئية أو الصوتية التي تقدم إلى المحكمة كدليل على ارتكاب جريمة، أو المشاركة في ارتكابها، ونحن هنا بصدد صورتين للتزييف أمام القضاء: الصورة الأولى: الدفاع السليبي ويكون من خلال الادعاء أمام القضاء بعدم مصداقية الأدلة المقدمة من فيديو أو تسجيل صوتي والادعاء بأنها من صنع التزييف العميق<sup>66</sup>، وهي ظاهرة خطيرة ترزع الأدلة الجنائية أمام القضاء حتى أطلق عليها الفقيهان تشيسني (Bobby Chesney) وسيترون (Danielle Citron) اسم «عائد الكذب» (Liar's Dividend)<sup>67</sup>، وتعني قيام الجاني بالدفاع أمام القضاء بأن المحتوى الذي يصوره وهو يقوم بارتكاب الجريمة مجرد تزييف عميق<sup>68</sup>، أما الصورة الثانية: فهي التزييف الإيجابي بحيث يقوم المتهم بتقديم دليل هو عبارة عن محتوى رقمي مزيف يظهره في مكان آخر بعيد عن مكان ووقت ارتكاب الجريمة<sup>69</sup>. وفي كلتا الصورتين نرى حجم الضرر الذي سوف ينال من الأدلة الجنائية وزعزعت للعدالة في قدرته على إحقاق العدالة.

### رابعاً: جرائم التزييف العميق ضد أمن واستقرار الدولة

بالنظر إلى طبيعة تقنية التزييف العميق، يمكن استخدامها من قبل قوى أجنبية أو محلية تسعى إلى زعزعة استقرار الدولة من خلال بث الفوضى، أو إثارة النعرات الطائفية سواء في أوقات الحروب أو السلم، فمثلاً خلال الغزو الروسي لأوكرانيا في عام 2022، ظهر الرئيس الأوكراني فولوديمير زيلينسكي في فيديو مزيف يطالب فيه قواته الاستسلام للروس<sup>70</sup>. ومن السيناريوهات المحتملة مثلاً تصوير أحد المسؤولين يتحدث ويطلب القوى الأمنية

64 R. Beckerman, et al. Adobe, The New York Times Company and Twitter Announce Content Authenticity Initiative to Develop Industry Standard for Content attribution (2019). <https://news.adobe.com/news//news-details/2019/Adobe-The-New-York-Times-Company-and-Twitter-Announce-Content-Authenticity-Initiative-to-Develop-Industry-Standard-for-Content-Attribution/default.aspx> (last visited July 20, 2023).

65 Chesney & Citron, supra note 2, p. 1760.

66 Dixon, supra note 4.

67 Chesney & Citron, note 2, p. 1753.

68 Ibid.

69 Brooks et al., supra note 1, p. 20.

70 Ibid.

بتشديد الرقابة على طائفة معينة من الشعب والتعامل معهم بشدة وهو ما يؤدي إلى إحداث بلبله في المجتمع، وقد يحدث العكس خلال الأوقات والظروف الاستثنائية كحالة غليان الشارع ضد سياسات الحكومة كالمظاهرات الشعبية ضد غلاء المعيشة بأن يستخدم التزييف العميق شخصية أحد رموز المعارضة وهو يطالب أتباعه أو مناصريه بالاعتداء على رجال الشرطة، وتدمير الممتلكات للتأثير على أصحاب القرار السياسي، أو خلال جائحة صحية يخرج وزير الصحة بفيديو مزيف يعلن إنهاء حالة الحظر وبثه عبر مواقع التواصل الاجتماعي والصفحات الإخبارية، وبالتالي إحداث كارثة وطنية. وقد تشكل تقنية التزييف العميق خطرًا على النظام الديمقراطي من خلال التأثير على أصوات الناخبين كما حدث في انتخابات الولايات المتحدة الأمريكية عام 2016 عندما قامت كل من الصين والاتحاد الروسي ببث أخبار مضللة على مواقع التواصل الاجتماعي ضد المرشحة الأمريكية السيدة هيلاري كلنتون<sup>71</sup>، كذلك تعرض الرئيس الأمريكي جو بايدن للعديد من الوجوه المزيفة في عام 2020 تظهره في حالات مبالغ فيها من التراجع المعرفي بهدف التأثير على الانتخابات الرئاسية. يشكل استخدام تقنية التزييف العميق أكبر خطورة لكونها أكثر إقناعًا وأكثر صعوبة في كشف حقيقتها، وقد عبر رئيس شركة ميكروسوفت في هذا الشأن براد سميث (Brad Smith) بأن تقنية التزييف العميق تشكل القلق الأكثر من بين تطبيقات الذكاء الاصطناعي الأخرى<sup>72</sup>. كذلك ليس ببعيد استخدام تقنية التزييف العميق كأحد الأسلحة في الحروب السيبرانية أو خلال التوتر السياسي بين دولتين أو أكثر؛ حيث قد تستخدم من قبل مجموعة مسلحة أو حزب معاد يرغب في إجبار دولة ما على اتخاذ قرارات سياسية من أجل التأثير على شعب تلك الدولة أو الحكومة فيها.

إن التكنولوجيا المستخدمة في تعديل وتزوير الصوت والصورة والفيديو تتطور بشكل سريع، ومن الأمور التي تترتب على شيوع استخدام هذه التقنية انعدام الثقة وزعزعة الحقائق وخداع حواس الإنسان الفطرية البصرية والسمعية، وبالتالي هناك حاجة إلى مواجهة جديدة رادعة في التعامل مع المحتوى الرقمي، ومعايير قانونية وعملية متقدمة ترافق هذه التقنيات الذكية للحد من الجرائم ومنع انتشارها.

### المطلب الثاني: مفهوم جرائم التزييف العميق

لدراسة مفهوم جرائم التزييف العميق نقسم هذا المطلب إلى فرعين نخصص الفرع الأول للمفهوم الطبيعي والاجتماعي للجريمة أولاً ومن ثم تطبيق تلك المفاهيم على جرائم التزييف العميق، ثم في الفرع الثاني نتناول المفهوم القانوني للجريمة ومن ثم تطبيق الأركان العامة للجريمة على جرائم التزييف العميق.

### الفرع الأول: المفهوم الطبيعي والاجتماعي لجرائم التزييف العميق

للجريمة أكثر من منظور كالمنظور الطبيعي (natural crime) الذي ابتدعه الفقيه الإيطالي (رافيل جاروفالو) ويتلخص في أن الجريمة هي كل فعل يجرح الحاسة الخلقية للمجتمع، غير أن الاهتمام انصب على المنظورين

71 Daniel et al., supra note 8.

72 D. Bartz, "Microsoft Chief Says Deep Fakes are Biggest AI Concern," Reuters (2023). <https://www.reuters.com/technology/microsoft-chief-calls-humans-rule-ai-safeguard-critical-infrastructure-2023-05-25/> (last visited July 16, 2023).

الاجتماعي والقانوني. فالمنظور الاجتماعي للجريمة وهو أكثر اتساعاً من المفهوم القانوني ينظر إلى الجريمة على أنها كل سلوك يتنافى مع القيم الاجتماعية السائدة في المجتمع وبالتالي ينظر إلى الجريمة كواقعة مادية إنسانية لا كواقعة قانونية مجردة<sup>73</sup>. أما من المنظور القانوني للجريمة فهي كل سلوك أو تصرف إيجابي نهى القانون عن إتيانه، أو أي تصرف سلبي نص القانون على إتيانه، وهذا المنظور هو الذي يرتب عقوبات جزائية على مرتكب الفعل بنص تشريعي صريح.

عند تطبيق مفهومي الجريمة الطبيعية والاجتماعية على ظاهرة فعل التزيف العميق، نجد أن هذا السلوك يحرف بوصلة إدراك الخير والشر لدى الإنسان السوي. إن ارتكاب فعل التزيف العميق يُعتبر سلوكاً شائناً وغير مقبول من قبل أفراد المجتمع، وبذلك يتعارض هذا الفعل مع القيم الاجتماعية المشتركة، التي تشمل رفض جميع أشكال الانحراف عن الطريق المستقيم وإحداث الأضرار المادية أو المعنوية للأفراد والمجتمع بأي وسيلة كانت.

الجريمة الطبيعية تشير إلى أن فعل التزيف العميق يتنافى مع الأخلاق والقيم الأخلاقية العامة؛ حيث يُعتبر تجاوزاً للسلوك الأخلاقي المتوقع من الأفراد. هذا السلوك يعتبر تجاوزاً لحدود الشرعية ويؤدي إلى إلحاق ضرر بالآخرين بطرق غير مقبولة. من ناحية أخرى، الجريمة الاجتماعية تشير إلى أن فعل التزيف العميق يؤثر على العلاقات الاجتماعية ويحل بالثقة والتفاهم بين أفراد المجتمع؛ حيث يمكن أن يؤدي هذا السلوك إلى تدهور العلاقات بين الأفراد وإحداث الأضرار المالية والجسدية والنفسية، وزعزعة استقرار المجتمع. إن هذا النوع من الجرائم يمكن أن يؤثر سلباً على القيم الاجتماعية المشتركة ويسهم في تفكك الأخلاق الاجتماعية والإخلال بالأمن والسلم المجتمعي، فجميع جرائم التزيف العميق تتعارض مع القيم الاجتماعية المشتركة التي تنادي بضرورة احترام الآخرين وعدم تعريض أفراد المجتمع للأذى أو الاعتداء عليهم أو على ممتلكاتهم بأي طريقة كانت أو تعريض السلم والأمن للخطر. وهو ما يمثل انحرافاً عن المسار الاجتماعي المقبول والشرعي ويتطلب تدخل القانون بنصوص صريحة للحد من انتشاره ومعاقبة المرتكبين له.

## الفرع الثاني: المفهوم القانوني والأركان الرئيسية لجرائم التزيف العميق

لدراسة المفهوم القانوني لا بد من عرض الأركان العامة للجريمة ومحاولة تطبيق هذه الأركان على جرائم التزيف العميق

### أولاً: الركن المادي

يتمثل الركن المادي للجريمة بشكل عام في المظهر الخارجي لنشاط الجاني الذي هو عبارة عن السلوك الإجرامي الذي يكون محلاً للتجريم والعقاب، فقانون العقوبات لا يعاقب على الأفكار والنيات الداخلية للإنسان، فلا يعاقب قانون العقوبات مثلاً على مجرد التفكير في ارتكاب الجريمة إلا إذا اقترن هذا التفكير بالخروج إلى العلن من خلال نشاط إيجابي مادي أو امتناع عن فعل، ولم يحدد المشرع الطريقة التي يمكن أن يلجأ إليها الجاني بارتكاب

73 طلال أبو عفيفة، أصول علمي الإجرام والعقاب واخر الجهود الدولية والعربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية، دار الجندي للنشر والتوزيع، القدس، 2013، ص 44.

الفعل<sup>74</sup>، وجرائم التزييف تتطلب القيام بتصرفات وأفعال إيجابية مادية وإن اتخذت الشكل غير المادي أو غير الملموس حيث يجب على المزييف العميق القيام بتصرفات وحركات من شأنها إحداث أثر خارجي ملموس يقع على نفسية الضحية أو أمواله أو سمعته أو إحداث ضرر على نطاق واسع بالمجتمع والدولة.

وبتطبيق الركن المادي على جرائم التزييف العميق يتضح أن الركن المادي لجريمة التزييف العميق يتكون من عنصرين:

1 - السلوك الإجرامي: ويتمثل في النشاط المادي الخارجي المكوّن للجريمة المتمثل في قيام الجاني بكامل إرادته باستخدام أحد تطبيقات التزييف العميق المتوفرة مجاناً أو المدفوعة الثمن على الشبكة الإلكترونية بتصميم وإنتاج المحتوى المزيف بعد أن يكون قد جمع المعلومات والبيانات الضرورية لإنتاج المحتوى، ثم تزويد التطبيقات الخاصة بالتزييف العميق بتلك المعلومات وإعطاء الأوامر الإلكترونية لإنتاج المحتوى، ثم العمل على إرساله وتداوله عبر مواقع التواصل الاجتماعي أو عبر المواقع المختلفة للشبكة الإلكترونية مثل اليوتيوب ومواقع الأخبار، أو استخدامه للحصول على منفعة مادية أو معنوية بطريقة غير مشروع كما هو الحال في جرائم الاحتيال العميق وجرائم التزييف ضد أمن واستقرار الدولة، لذلك تتمثل طبيعة السلوك الإجرامي في جرائم التزييف العميق في قيام الجاني بفعل إيجابي من خلال استخدام وتوجيه واستغلال تطبيقات التزييف العميق بشكل غير مشروع لإحداث الضرر بالضحية، هذا ولا يمكن أن تقع الجريمة بفعل سلبي مثل الامتناع عن القيام بفعل.

ويلاحظ أنّ طبيعة السلوك الإجرامي في هذا النوع من الجرائم قد تتخذ أشكالاً عدة على النحو التالي: فالجريمة قد تتخذ سلوكاً إجرامياً وقتياً يبدأ وينتهي حالاً مثل جرائم الاحتيال العميق حيث يستعمل الجاني المحتوى المزيف للإيقاع بالضحية والحصول على المال، وقد تتخذ الجريمة شكل جريمة مستمرة تبدأ منذ إنشاء المحتوى المزيف واستمرار تداوله على المواقع الإلكترونية، فسلوك الجاني في هذه الحالات يستمر لوقت طويل يعاني الضحية خلاله ألماً نفسياً وقد يترتب عليه قيام الضحية بإيذاء النفس كنتيجة للتخلص من هذا الألم والعار الذي يشعر به جراء الابتزاز والانتقام الإباحي أو تشويه السمعة إلى جانب الأضرار المادية وفقدان الثقة بمؤسسات الدولة الذي قد يستمر لفترة من الزمن في جرائم التزييف العميق ضد الدولة.

2 - النتيجة المترتبة على السلوك الإجرامي: تعتبر النتيجة العنصر الثاني من عناصر الركن المادي للجريمة ويقصد بها الأثر المترتب على السلوك الإجرامي، ويوجد مفهومان للنتيجة، هما:

أ - المفهوم المادي: يقصد بالنتيجة في هذا المفهوم الأثر أو التغيير الحسي والملموس الذي يحدثه السلوك الإجرامي في العالم الخارجي. وقد أثبتت جميع الدراسات والأبحاث بما لا يدعو إلى الشك الآثار الجسدية والخطيرة التي قد تترتب على هذا النوع من الجرائم، ففي الجرائم التي تستهدف الأشخاص

74 عبد العزيز أحمد الحسن، شرح قانون الجرائم والعقوبات الاتحادي لدولة الإمارات العربية المتحدة الصادر بموجب المرسوم بقانون اتحادي رقم 31 لسنة 2021: الأحكام العامة - الكتاب الأول - النظرية العامة للجريمة، دار النهضة العلمية، دبي، 2022، ص 142.

يعاني الضحية من القلق والإحباط والحزن والغضب وما يلحق ذلك من آثار سيئة على الأسرة خصوصًا وتدهور العلاقات والثقة بين الأفراد والمؤسسات الخاصة أو العامة أو الخسائر المادية، أما الجرائم التي تستهدف المجتمع والدولة فتحدث أضرارًا جسيمة في وظائف الدولة وتعكير الصفو والأمن العام في الدولة والثقة بمؤسساتها.

ب. المفهوم القانوني: يقصد بالنتيجة في هذا المفهوم ما يسببه السلوك الإجرامي من ضرر أو خطر يصيب أو يهدد مصلحة محمية قانونًا وهو بهذا المعنى عنصر هام وضروري لا تقوم الجريمة بدونه<sup>75</sup>، وهذا النوع من الجرائم قد يترتب عليه العدوان على الحقوق الشخصية والمالية للأفراد والمؤسسات الخاصة والعامة، وكذلك الاعتداء على سمعة الدولة ومكانتها.

ووفقًا للمفهوم القانوني للنتيجة وبالنظر إلى الصورة التي تتخذها الجريمة قسم الفقهاء الجرائم إلى نوعين:

1 - النوع الأول: جرائم الضرر وهي التي تتخذ فيها النتيجة الجرمية صورة إلحاق اعتداء فعلي بالضحية وهي متحققة في جرائم التزييف العميق كإحداث الأضرار النفسية والمادية في جرائم الابتزاز وتشويه السمعة والاحتيال كما أشرنا سابقًا.

2 - النوع الثاني: جرائم الخطر وهي التي تكون فيها النتيجة الإجرامية بالاعتداء محتملة، فالقانون هنا لا يستلزم لتحقيق النتيجة وقوع ضرر بالفعل بل يكفي مجرد إحداث الخطر، فيمثل الخطر هنا النتيجة المترتبة على السلوك الإجرامي وهي بهذا المعنى متحققة في جرائم التزييف العميق مثل جريمة التأثير على سير الانتخابات وضد الصحافة والإعلام.

ويلاحظ أن جرائم التزييف العميق ينتج عنها ضرر عام وضرر خاص، أما الضرر العام فيتمثل في حالة الإضرار برجال الدولة والانتخابات وزعزعة الثقة في مؤسسات الدولة والقضاء مما يشكل اضطرابًا في أمن المجتمع وكيانه وإثارة القلاقل والرعب والغضب في المجتمع، وأما الضرر الخاص فهو الضرر الذي يصيب المجني عليه بشكل مباشر والضرر غير المباشر الذي يصيب عائلة الضحية جراء المعاناة المتحققة من نشر المحتوى المزيف الذي يجرح الشعور ويسبب الكثير من الألم.

### ثانيا: الركن المعنوي

أما الركن المعنوي لجرائم التزييف العميق فيبنى على كونها من الجرائم العمدية التي تقوم على القصد الجنائي العام بعنصره العلم والإرادة؛ إذ يجب أن يعلم الجاني أن ما يقوم به هو تزييف باستخدام أحد تطبيقات تقنية التزييف العميق لصور وأصوات إنسان حي بهدف توليد المقطع المزيف ودون موافقة صاحب المحتوى الأصلي أو من يتم تزييف شخصيته، وأن تكون إرادته حرة متجهة إلى إحداث هذا السلوك. ولا تهم بعد ذلك الأهداف التي سعى إليها الجاني سواء كانت تحقيق الربح المادي أو الانتقام من الضحية أو تحقيق مآرب سياسية أو مجرد الفضول والتسلية.

75 الحسن، هامش 74.

## المبحث الثاني: مواجهة جرائم التزييف العميق

في عصر الذكاء الاصطناعي والتطور التكنولوجي، أصبح التزييف العميق يشكل تحديًا على جميع الأصعدة؛ حيث وجدت كثير من الدول أنفسها في سباق مع الزمن لإصدار تشريعات وأحكام خاصة بالتزييف العميق لمنع الاستخدامات السلبية أو الحد منها، والنص على عقوبات رادعة دون المساس بالحق في الإبداع وحرية التفكير والتعبير وخلق البيئة المناسبة لتطور التقنية واستخداماتها المفيدة. ومما لا شك فيه أن مكافحة جرائم التزييف العميق هي عملية مشتركة لا تستطيع الحكومات أو الشركات مواجهتها بشكل منفرد وبالتالي لا بد من تضافر جهود الحكومات، والشركات المنتجة والمطورة لهذه التقنية إلى جانب دور المجتمع المدني.

وبناء على ذلك، يمكن لنا حصر المواجهة في عدة اتجاهات:

### المطلب الأول: المواجهة القانونية

تعتمد المواجهة القانونية في الأساس على توظيف القوانين السارية لمكافحة الجرائم بشكل فعال أو العمل على سن قوانين جديدة لمكافحة الظواهر الحديثة بعد أن تعجز القوانين السارية عن فعل ذلك، وقد ثبت قبل عدة عقود وتحديدًا في مطلع الثمانينات من القرن المنصرم عدم كفاية أو فاعلية القوانين التقليدية لمكافحة أو مواجهة الجرائم السيبرانية، مما دعا المشرع في معظم الدول إلى إصدار قوانين خاصة تناسب تلك الجرائم، وهنا نطرح السؤال التالي: ما مدى كفاية القوانين السيبرانية في مواجهة كافة أشكال جرائم التزييف العميق بشكل فعال أم أن الحاجة ماسة لنصوص جديدة؟

### الفرع الأول: المواجهة القانونية باستخدام قوانين الجرائم الإلكترونية

تم إصدار تشريعات خاصة في معظم الدول لتجريم الجرائم الإلكترونية، وذلك لمواجهة التحديات التي تطرحها هذه الجرائم وحماية الأفراد والمؤسسات الخاصة والعامة في الدولة، وقد شهدت هذه القوانين العديد من التعديلات لتواكب تطورات الجريمة الإلكترونية، فمثلًا أصدر المشرع الأردني أول قانون للجرائم الإلكترونية عام 2010، ولعجز هذا القانون عن مواكبة التطورات في مجال الجرائم الإلكترونية، أصدر قانونًا جديدًا عام 2015 تحت مسمى قانون الجرائم الإلكترونية لعام 2015، ثم في عام 2023 أصدر قانونًا جديدًا ليحل محل قانون 2015، بعد أن اتضح قصوره في معالجة الجرائم الإلكترونية، ونجد لأول مرة استخدام المشرع الأردني في هذا القانون ما يشير إلى إحدى جرائم التزييف العميق بشكل غير مباشر حيث نص في الفقرة الثانية من المادة (20) بالقول «يعاقب ... كل من استخدم شبكة معلوماتية أو تقنية المعلومات أو نظام المعلومات أو موقعًا إلكترونيًا أو منصة تواصل اجتماعي لإجراء تركيب أو تعديل أو معالجة على تسجيل أو صورة أو مشهد أو فيديو لما يحرص الشخص على صونه وعدم إظهاره للعامة بقصد التشهير أو الإساءة أو الحصول على منفعة من جراء ذلك»<sup>76</sup>، ومن الممكن استخدام هذا النص لتجريم بعض أشكال جرائم التزييف العميق مثل جرائم الابتزاز والانتقام الإباحي العميق، لكن المادة المذكورة لا تظال الجرائم الأخرى والتي لا تستهدف ما يحرص الشخص على صونه وعدم

76 قانون الجرائم الإلكترونية الأردني لسنة 2023.

إظهاره للعامة. وكذلك أصدر المشرع الإماراتي عدة قوانين سيرانية كان آخرها قانون رقم (34) لسنة 2021 لمكافحة الشائعات والجرائم الإلكترونية، وبالرجوع إلى هذا القانون نلاحظ خلوه من الإشارة إلى جرائم التزييف العميق، لكن تضمن بعض المواد التي يمكن أن تجرم هذا النوع من الجرائم بصورة غير مباشرة؛ حيث نصت المادة (16) على أنه «يعاقب... كل من حاز أو أحرز أو أعد أو صمم أو أنتج أو استورد أو أتاح أو استخدم أي برنامج معلوماتي أو وسيلة تقنية معلومات أو أكواد مرور أو رموزاً أو استخدم التشفير بقصد ارتكاب أي جريمة من الجرائم المنصوص عليها في هذا المرسوم...»<sup>77</sup>، ومن هذه الجرائم التي نص عليها القانون جرائم التحريض على المساس بأمن الدولة المادة (23)، وكذلك المادة (24) الترويج لإثارة الفتنة والإضرار بالوحدة الوطنية، وجرائم الابتزاز والتهديد الإلكتروني المادة (42)، وكذلك الفقرة الخامسة من نص المادة (44) التي تجرم القيام بأي تعديل أو معالجة على تسجيل أو صورة أو مشهد، بقصد التشهير أو الإساءة إلى شخص آخر. كذلك جرم المشرع القطري في المادة رقم (8) من قانون مكافحة الجرائم الإلكترونية رقم (14) لسنة 2014 كل من تعدى على أي من المبادئ أو القيم الاجتماعية، أو نشر أخباراً أو صوراً أو تسجيلات صوتية أو مرئية تتصل بحرمة الحياة الخاصة أو العائلية للأشخاص، ولو كانت صحيحة، أو تعدى على الغير بالسب أو القذف، عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات<sup>78</sup>. ونحن نرى، وبالرغم من إمكانية استخدام هذه النصوص لتجريم بعض أشكال جرائم التزييف العميق، أنها قاصرة عن تقديم نصوص خاصة وشاملة تعالج كافة جوانب استخدامات تقنية التزييف العميق إلى جانب عدم الإشارة في تلك النصوص من قريب أو من بعيد إلى الأطراف الأخرى التي لها علاقة بشكل مباشر أو غير مباشر بجرائم تقنية التزييف العميق، فمثلاً لا تعالج هذه القوانين دور الشركات المنتجة لتقنية التزييف العميق في الحد من جرائم التزييف العميق، أو دور مزودي الخدمة، وكذلك ليست هناك إشارة إلى تداول أو إعادة نشر المحتوى المزيف، وليست هناك إشارة إلى حقوق صاحب المحتوى الحقيقي الذي تم استخدامه لإنتاج المحتوى المزيف، هذا بالإضافة إلى غياب تفصيل دقيق لتلك الجرائم والإجراءات الوقائية أو العلاجية لها كما فعل المشرع في بعض الدول الأخرى بالنص صراحة على مكافحة تلك الجرائم.

### الفرع الثاني: المواجهة القانونية باستخدام قوانين التزييف العميق

المواجهة القانونية من أهم أدوات الردع عن الاستخدام السلبي لهذه التقنية والتصدي لها والحد من حالات الإفلات من العقاب العادل الذي يناسب جسامة الفعل. وتعتبر جمهورية الصين الشعبية من أوائل الدول التي أصدرت عدداً من التشريعات والأحكام التي تنظم الذكاء الاصطناعي بشكل عام وتقنية التزييف العميق بشكل خاص<sup>79</sup>، ففي نهاية عام 2022 أصدرت إدارة الأمن المعلوماتي بالتعاون مع وزارة الصناعة والتكنولوجيا ووزارة الأمن العام الصيني نظاماً يسمى «أحكام إدارة خدمات معلومات الإنترنت للتزييف العميق» (Provisions on the Administration of Deep Synthesis (Internet Information Services)). يتكون من 25 مادة تتعلق

77 قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي رقم (34) لسنة 2021.

78 قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014.

79 D. Laje, "China's Deep Fake Law Is Fake," (2023). <https://www.afcea.org/signal-media/cyber-edge/chinas-deep-fake-law-fake> (last visited Aug 24, 2023).

باستخدام تقنية التزييف العميق التي دخلت حيز التنفيذ في 10 يناير 2023، ومن أهم ما نص عليه النظام<sup>80</sup>: أنه لا يجوز لأي منظمة أو فرد استخدام خدمات التزييف العميق لإنتاج أو نسخ أو نشر أو نقل المعلومات المحظورة بموجب القوانين واللوائح الإدارية، مثل تعريض الأمن والمصالح الوطنية للخطر، أو الإضرار بصورة الوطن، أو انتهاك المصلحة العامة، أو تعكير النظام الاقتصادي والاجتماعي، أو انتهاك الحقوق والمصالح القانونية للآخرين أو نشر الأخبار الكاذبة<sup>81</sup>. كذلك نص النظام على عدد من الالتزامات تقع على عاتق مزودي خدمات تقنية التزييف العميق لعل من أهمها مسؤولية مزود خدمات تقنية التزييف العميق عن تأمين أمن وسلامة المعلومات والبيانات الخاصة بالمستخدمين وتسجيلهم بالاسم الحقيقي ومنع الاحتيال<sup>82</sup>، كذلك ألزم النظام مزود الخدمة بالتحقق من هوية المستخدمين لتقنية التزييف العميق<sup>83</sup>، أما المادة 11 فقد ألزمت مزود الخدمة اتخاذ تدابير فورية في حال اكتشاف محتوى مزيف يخالف أحكام القانون الصيني من ضمن هذه التدابير دحض ما ورد في المحتوى وحفظ سجل لذلك المحتوى ثم إبلاغ السلطات المختصة<sup>84</sup>. وعلى المزود أن يضع علامة مائية (Watermark)<sup>85</sup> على المحتوى بشكل لا يعيق استخدام التقنية<sup>86</sup>. وبالرغم من أهمية هذا النظام والأهداف التي يسعى إلى تحقيقها<sup>87</sup> فإنه يواجه تحديات وصعوبات كبيرة تتعلق بآلية تطبيقه وغموضه وصعوبة تفسيره وهو ما أدى إلى تعرضه للنقد<sup>88</sup>، في مقابل ذلك أعرب بعض الساسة في الولايات المتحدة عن القلق من أن تصبح الصين وقوانينها في هذا الشأن النموذج لدول العالم<sup>89</sup>. وبالنظر إلى القانون التقليدي نجد أن المادة 181 من قانون العقوبات الصيني تعاقب بالحبس كل من يزيف وينشر معلومات كاذبة بهدف التأثير السلبي على سوق الأسهم وإثارة الفوضى في سوق تداول الأسهم<sup>90</sup>، كذلك نص في المادة 221 على حبس كل من يقوم بتزوير معلومات كاذبة ونشرها عبر الشبكات المعلوماتية أو

80 China Law Translate, Provisions on the Administration of Deep Synthesis Internet Information Services, 2023. <https://www.chinalawtranslate.com/en/deep-synthesis>. (last visited Aug 24, 2023).

81 Article 6 of the Provisions on the Administration of Deep Synthesis Internet Information Services.

82 Article 7 of the Provisions on the Administration of Deep Synthesis Internet Information Services.

83 Article 9 of the Provisions on the Administration of Deep Synthesis Internet Information Services.

84 Article 11 of the Provisions on the Administration of Deep Synthesis Internet Information Services.

85 العلامة المائية عبارة عن علامة مرئية أو غير مرئية تضاف إلى صورة أو فيديو للإشارة إلى مالكيها أو مصداقيتها وهي تستخدم عادة لمنع التلاعب بالمحتوى الإلكتروني، وقد تتخذ شكل نص أو رمز أو نمط معيناً ضمن المحتوى الرقمي، وقد طور الخبراء علامة مائية ذكية خاصة للتزييف العميق بحيث تتعرف على الفيديو المزيف ليظهر بصورة أقل وضوحاً من المحتوى الأصلي. للمزيد:

L. Luo Chen, Smart Watermark to Defend against Deepfake Image Manipulation, In IEEE 6th International Conference on Computer and Communication Systems (2021), pp. 380-384. <https://doi.org/10.1109/ICCCS52626.2021.9449287>

86 المادة رقم 16 من نظام أحكام إدارة خدمات معلومات الإنترنت للتزييف العميق.

87 Cyberspace Administration of China. The Cyberspace Administration of China and other three departments issued the Provisions on the Administration of Deep Synthesis of Internet Information Services (2022). [http://www.cac.gov.cn/202211/12-/c\\_1672221949318230.htm](http://www.cac.gov.cn/202211/12-/c_1672221949318230.htm) (last visited August 24, 2023).

88 Laje, Supra note 79.

89 M. Sheehan, China's AI Regulations and How they Get Made (July 10, 2023), Carnegie Endowment for International Peace, Publications Department, 1779 Massachusetts Avenue NW.

90 Article 181 Criminal Law of the People's Republic of China 1997.

مواقع التواصل الاجتماعي بقصد النيل من النظام العام أو التشهير بالآخرين<sup>91</sup>. من كل ذلك يتضح أن المشرع الصيني أنشأ أدوات قانونية رادعة في هذا المجال تخدم سبل مكافحة وتحد من انتشار الاستخدام السلبي.

وعلى مستوى الاتحاد الأوروبي يمكن تطبيق نوعين من أدوات المواجهة القانونية لمكافحة التزييف العميق: فقد طرح الاتحاد في شهر أبريل من عام 2021 المقترح التنظيمي للذكاء الاصطناعي (AI Regulatory Framework) (Proposal)، وهو عبارة عن إطار قانوني مقترح من قبل المفوضية الأوروبية لمعالجة مخاطر الذكاء الاصطناعي، وقد عرض للنقاش في البرلمان الأوروبي في شهر يونيو من عام 2023؛ حيث يصنف المقترح منتجات الذكاء الاصطناعي المختلفة على أساس الخطورة الى أربعة مستويات على النحو الآتي:

- المستوى الأول: خطورة غير مقبولة وضمن هذا المستوى تشكل منتجات الذكاء الاصطناعي خطورة على معاش وسلامة الأفراد والحقوق التي يكفلها نظام الاتحاد الأوروبي لمواطنيه، وبناء على ذلك يمنع التعامل أو إنتاج أو طرح أي من منتجات الذكاء الاصطناعي في دول الاتحاد التي تصنف ضمن بند الخطورة غير المقبولة<sup>92</sup>.
- المستوى الثاني: خطورة عالية حيث تخضع المنتجات الذكية لقواعد صارمة في التعامل كوجوب تسجيل المنتج لدى قاعدة البيانات الأوروبية.
- المستوى الثالث: متوسط الخطورة أو خطورة محدودة؛ حيث تخضع منتجات الذكاء الاصطناعي لقواعد محددة، وتقع ضمن هذه المنتجات الذكية تقنية التزييف العميق.
- المستوى الرابع: خطورة منخفضة أو ضئيلة؛ حيث لا يخضع هذا النوع من المنتجات إلى قيود.

وحيث صُنفت تقنية التزييف العميق ضمن المستوى الثالث، فقد نص المقترح التنظيمي في المادة (52) الفقرة الثالثة على وجوب قيام المستخدم لتقنية التزييف العميق بالتصريح بحقيقة المحتوى المزيف ما لم يكن الاستخدام لأغراض مشروعة تتعلق بكشف أو منع الجريمة أو التحقيق الجنائي ومحاكمة المجرمين<sup>93</sup>. ويؤخذ على المقترح عدم إدراج أي عقوبات على مخالفة المادة سالفه الذكر أو النص على تعويضات للمجني عليه.

أما الأداة القانونية الأخرى التي يمكن استخدامها لمكافحة جرائم التزييف العميق على مستوى الاتحاد الأوروبي فهي اللائحة العامة لحماية البيانات (General Data Protection Regulation)؛ حيث تنص على اعتبار البيانات من فيديو وصور وصوت التي تستخدم في التزييف العميق من البيانات التي تخضع للحماية، وبالتالي يجب أن تخضع استخدامات التزييف العميق لشروط محددة بهدف حماية الخصوصية والبيانات الشخصية، وهذه الشروط تتمحور حول وجوب توفر مصلحة مشروعة لدى منتج المحتوى المزيف عند إنتاج الفيديو، أو الحصول على موافقة الشخص الذي يتم استخدام صورته أو بياناته أو صوته لصنع المحتوى المزيف، إلى جانب موافقة

91 Zhang, Supra note 41.

92 T. Madiega, Artificial Intelligence Act, EPRS | European Parliamentary Research Service (2023).

93 Huijstee, Supra note 17.

الشخص صاحب الفيديو الأصلي.

أما في الولايات المتحدة الأمريكية فحتى تاريخ كتابة هذا البحث لا يوجد قانون فيدرالي يعالج جرائم التزييف العميق بشكل كلي كما هو الحال في النظام الصيني، فهناك قانون مقترح على المستوى الفيدرالي تقدم به عضو الكونجرس الأمريكي السيدة يفيت كلارك (Yvette Clarke)<sup>94</sup> يسمى قانون «مساءلة التزييف العميق» (DEEP FAKES Accountability Act 2020)<sup>95</sup> يهدف إلى تنظيم صناعة تكنولوجيا التزييف العميق وحماية المجتمع الأمريكي والنظام العام في الدولة من جرائمه وسوء استخدامه، وقد تضمن القانون المقترح الأحكام الرئيسية التالية:

أولاً: يلزم القانون بأن يكون لأي فيديو أو صوت مزيف علامة مائية رقمية<sup>96</sup> وأن يتضمن إعلاناً صوتياً<sup>97</sup> ونصاً صريحاً مكتوباً<sup>98</sup> يشير إلى أن المحتوى من إنتاج تقنية التزييف العميق. وبالنتيجة إذا لم يتضمن المحتوى ذلك يعد جريمة يعاقب عليها القانون بالغرامة أو الحبس لمدة لا تزيد على خمس سنوات أو كلا العقوبتين<sup>99</sup>.

ثانياً: أنشأ القانون عقوبة مدنية قيمتها 150 ألف دولار على كل من يخالف أحكام المواد السابقة وكذلك التعويض عن أي ضرر يسببه المحتوى المعدل<sup>100</sup>.

ثالثاً: يلزم القانون المدعي العام الأمريكي بتعين منسق في كل مكتب من مكاتب الادعاء العام في كل ولاية أمريكية تكون مهمته استقبال الشكاوى من المواطنين حول أي محتوى مزيف متداول من إنتاج دولة أجنبية أو وكلائها ويقوم هذا المنسق بمتابعة الإجراءات القضائية ضد تلك الجهة<sup>101</sup>.

رابعاً: يلزم القانون الشركات التكنولوجية الأمريكية التي تنتج تقنية التزييف العميق أن يكون من ضمن خصائص التطبيق أو التقنية تضمينها العلامة المائية ومعلومات حول شروط الاستعمال وبيان المسؤولية القانونية الجزائية والمدنية الواردة في القانون<sup>102</sup>.

94 U.S. Congress. (n.d.). H.R.3230 - DEEP FAKES Accountability Act. <https://www.congress.gov/bill/116th-congress/house-bill/3230> (last visited Aug 26, 2023).

95 The «DEEP FAKES Accountability Act» stands for "Defending Each and Every Person from False Appearances by Keeping Exploitation Subject to Accountability Act."

اشتق اسم قانون مساءلة التزييف العميق من عنوانه من بداية كل حرف من الاسم الكامل لهذا القانون «الدفاع عن كل شكل من المظاهر الكاذبة من خلال إبقاء الطرف المستغل محل المساءلة القانونية».

96 Article 1041 Sec 2B DEEP FAKES Accountability Act 2020.

97 Article 1041 Sec 2C (1) DEEP FAKES Accountability Act 2020.

98 Article 1041 Sec 2C (2) DEEP FAKES Accountability Act 2020.

99 Article 1041 Sec 2F (1) DEEP FAKES Accountability Act 2020.

100 Article 1041 Sec 2F (2) DEEP FAKES Accountability Act 2020.

101 Article 1042 Sec 2 A DEEP FAKES Accountability Act 2020.

102 Article 1042 Sec 3 (1) (2) A DEEP FAKES Accountability Act 2020.

خامساً: يدعو القانون إلى إنشاء قوة تنفيذية لدى وزارة الأمن الداخلي لكشف ومكافحة جرائم التزييف العميق<sup>103</sup>.

يتضح من ذلك أن المشرع الصيني والأوروبي والأمريكي لم يكتفوا بالقوانين التقليدية أو السيرانية لمواجهة ظاهرة التزييف العميق إيماناً منهم بقصور تلك القوانين في مواجهة فعالة لتقنية قد تستخدم بشكل سلبي بطريقة لم يسبق لها مثيل أو رغبة من المشرع في تحديد حجم العقوبات والتعويض عن جرائم التزييف العميق كما فعل المشرع الأمريكي. فالقانون الصيني والمقترح الأمريكي يؤديان دوراً هاماً في تأمين الإجراءات الوقائية والجزائية التي تمنع إنتاج التزييف العميق لأغراض إجرامية من خلال تفعيل دور مزود الخدمة وإلزام المنتج باتخاذ الإجراءات الضرورية لكشف التزييف، كذلك يحققان الردع من خلال الإشارة إلى الجرائم والعقوبات المترتبة على الاستخدام السلبي للتقنية. أما المشرع الأوروبي فقد كان أقل وضوحاً بعدم النص صراحة على جرائم التزييف العميق وعدم تضمين كل من المقترح التنظيمي للذكاء الاصطناعي واللائحة العامة لحماية البيانات كافة وضع الالتزامات على عاتق المنتج ومزود الخدمة إلى جانب غياب العقوبات في حال مخالفة تلك الأنظمة وخصوصاً خلو المقترح التنظيمي للذكاء الاصطناعي من تحديد العقوبات الجزائية.

وعلى كون التزييف العميق من الجرائم العابرة للحدود وحتى يتم منع وضبط وردع الاستخدام السيئ لهذه التقنية على جميع الدول تبني قوانين جديدة تعالج مسائل التزييف العميق كما فعل المشرعان الصيني والأمريكي ونحن بدورنا هنا نحث المشرع الوطني على إعداد مشروع قانون يخصص استخدامات هذه التقنية بتحديد العقوبات والتعويض عن الأضرار التي يمكن أن تترتب على الاستخدام السلبي لهذه التقنية، ويضع التزامات على عاتق المنتجين ومزودي الخدمات لمنع وإزالة المحتوى المزيف، والنص على ضرورة استحداث أجهزة متخصصة ضمن أقسام مكافحة الجرائم الإلكترونية للتعامل المباشر مع ضحايا هذا النوع من الجرائم واتخاذ الإجراءات الفورية لإزالة المحتوى.

### المطلب الثاني: المواجهة باستخدام أدوات الذكاء الاصطناعي

بالرغم من كون برامج التزييف العميق تعطي صورة عالية الدقة وواقعية إلا أنه تمكن معرفة الأصل من خلال استخدام عدد من الأدوات والبرامج التكنولوجية<sup>104</sup>؛ حيث يؤكد الباحثون في مجال الذكاء الاصطناعي وجود تنافس محموم بين تقنيات التزييف العميق وتقنيات الكشف، حتى وصف هذا التنافس بـ «لعبة القط والفأر»، وهي إشارة إلى التحسينات التي تطرأ على تقنية التزييف العميق لتلحق بها تقنيات الكشف عنه<sup>105</sup>. في مقابل ذلك يؤكد بعض الباحثين أن تقنيات وتطبيقات التزييف تتطور باستمرار وبسرعة تجعل من اكتشافه أمراً صعباً في المستقبل

103 Article 918 Sec 7 (A) A DEEP FAKES Accountability Act 2020.

104 Y. Li & S. Lyu, «Exposing DeepFake videos by detecting face warping artifacts,» (2018). Cornell University. <https://arxiv.org/pdf/1811.00656.pdf> (last visited May 24, 2023)

105 R. Tolosana, et al., Future trends in digital face manipulation and detection, in C. Rathgeb et al. (Eds.), Handbook of Digital Face Manipulation and Detection: From DeepFakes to Morphing Attacks 463 (Springer 2022).

القريب<sup>106</sup>، وبالرغم من هذا التأكيد تبقى تقنيات الكشف أحد أهم الخيارات في مكافحة جرائم التزييف العميق، ويكون ذلك من خلال استخدام أدوات الذكاء الاصطناعي لتطوير خوارزميات قادرة على اكتشاف وتحديد محتوى التزييف العميق في العالم الافتراضي، ومن خلال التطوير المستمر لأنظمة آلية قادرة على مراقبة وتحليل المنصات الإلكترونية لكشف محتوى التزييف العميق، ثم العمل على إزالته في الوقت المناسب ومنع انتشاره<sup>107</sup>. وقد ألزمت بعض مواد القانون الصيني والأمريكي الخاص بالمسؤولية عن التزييف العميق الشركات التكنولوجية المنتجة والمطورة لتقنية التزييف العميق بتبني سياسات وإجراءات تحد وتمنع من استخدامها لأغراض غير قانونية كما بينا في المطلب الأول.

### المطلب الثالث: المواجهة بإجراءات من جانب القطاع الخاص والإعلام

تلعب الشركات التكنولوجية العملاقة مثل شركات جوجل (Google) وميتا (Meta) وأكس (X) وتيك توك (TikTok) وغيرها من شركات منتجة للذكاء الاصطناعي أو مستخدمة له دورًا كبيرًا في إدارة مكافحة صناعة التزييف العميق؛ حيث أصدرت كل من تلك الشركات إجراءات للقضاء على نشر المحتوى المزيف فمثلًا في التاسع من مايو 2023 قامت شركة دويين (Douyin) وهو تطبيق مشابه لتطبيق تيك توك لكن بالنسخة الصينية بعدد من الإجراءات لمكافحة المحتوى المزيف، ومن أهم تلك الإجراءات إلزام الناشرين بوضع علامة فارقة تميز المحتوى الحقيقي عن المزيف، ويتحمل الناشر والمسؤولية عن الأضرار الناتجة عن المحتوى، كذلك يمنع بشكل قاطع استخدام التقنية بما يخالف أحكام القانون السائد، كما تلزم الإجراءات المستخدمين بتسجيل الشخصية الافتراضية (Avatar) والتحقق من الشخصية الحقيقية لصاحب الشخصية الافتراضية<sup>108</sup>. في المقابل وفرت شركة جوجل (Google) وميتا (Facebook) للباحثين قاعدة بيانات ضخمة تحتوي على فيديوهات مزيفة وحقيقية بهدف مساعدة الباحثين على تطوير تقنيات الكشف عن المحتوى المزيف<sup>109</sup>. وقد أطلقت شركة ميتا بالتعاون مع شركة أمازون وميكروسوفت وعدد من الجامعات ومراكز البحث العلمي في الولايات المتحدة الأمريكية عددا من الحوافز والجوائز والدعم المالي للباحثين لتطوير وسائل الكشف عن المحتوى المزيف<sup>110</sup>. من جهة أخرى تلعب شركات الإعلام العالمية دورًا كبيرًا في مكافحة ظاهرة التزييف العميق حيث أطلقت شركة الإعلام نيويورك تايمز بالتعاون مع شركة أدوبي (Adobe) وشركة أكس (تويتر سابقًا) مبادرة أصالة المحتوى (Content Authenticity Initiative) وتهدف إلى إنشاء معايير موحدة تطبق على الصناعة الرقمية للتحقق من أصالة المحتوى<sup>111</sup>، حيث أكد مدير البرامج في مؤسسة وتنس (WITNESS) على أهمية دور الصحافة في مكافحة الظاهرة من خلال قيام

106 Ibid.

107 Pantserev, supra note 16.

108 Zhang, supra note 41.

109 Vizoso, Vaz-Álvarez and López-García, supra note 22.

110 K. Wiggers, Facebook, Microsoft and Others Launch Deepfake Detection Challenge. VentureBeat. <https://venturebeat.com/ai/facebook-microsoft-and-others-launch-deepfake-detection-challenge/> (last visited Aug 25, 2023).

111 L. Rosenthal, et al., The Content Authenticity Initiative: Setting the Standard for Digital Content Attribution, CAI, August 2020.

الصحفيين بتقديم دليل للمشاهدين على صحة ما ينشرون وعلى أهمية تبني أسلوب سفت (SIFT)، وهو عبارة عن اختصار (توقف، تحقق، ابحث عن تغطية أفضل، اعثر على مصدر الادعاء) وهذه سلسلة من الإجراءات تحتم على الصحفي اتخاذها قبل نشر الخبر مما يؤدي إلى نشر محتوى مضمون وليس مزيفاً<sup>112</sup>، وفي هذا السياق تبنت شركة أكس (X) استراتيجية من أربع خطوات الأولى تتمثل في إصدار إشعار في حالة بث محتوى مزيف ثم إصدار تحذير بأنه مزيف قبل النشر وفي الخطوة الثالثة تضمن المحتوى المزيف رابطاً يقود المشاهد إلى مصدر المحتوى الذي يشير إلى: لماذا وكيف تم تزييف المحتوى الحقيقي، أما الخطوة الأخيرة فتتمثل في إزالة كل المحتويات المزيفة التي تشكل خطراً أو تهدد حياة الآخرين<sup>113</sup>.

## خاتمة

تعد ظاهرة التزييف العميق من الظواهر المستحدثة مع تأكيد الباحثين على انتشارها في المستقبل القريب حيث تمثل جانباً من ثورة الذكاء الاصطناعي التي باتت تسيطر على كثير من القطاعات، وكغيرها من التقنيات الحديثة التي يمكن أن تقدم للبشرية الكثير من الفوائد على جميع المستويات التعليمية والترفيهية والتجارية، فهي سلاح ذو حدين تحمل في طياتها الكثير من المخاطر وقد تصبح أداة جريمة خطيرة متوفرة وسهلة الوصول والتكلفة في يد المجرمين مسببة الأضرار الجسيمة للأفراد والمؤسسات والممتلكات وحتى زعزعة استقرار الأمن الوطني للدول، وكل ذلك يستدعي التسليح بأدوات المكافحة القانونية والتكنولوجية والمجتمعية وتضافر الجهود بين القطاع الخاص والعام في الدول لمنع ومكافحة سوء الاستخدام. ومن خلال هذا البحث، نخلص إلى النتائج والتوصيات الآتية:

### أولاً: النتائج

- تقنية التزييف العميق سلاح ذو حدين إيجابي مفيد وسلبى ضار يمكن استخدامها لارتكاب العديد من الجرائم التقليدية بأسلوب حديث.
- تعتبر ظاهرة التزييف العميق الجرمي من الظواهر الإجرامية التي قد تسبب الكثير من الأضرار للأفراد والمؤسسات والدول.
- لم تأت تقنية التزييف العميق بجرائم جديدة لكنها أداة حديثة لارتكاب العديد من الجرائم التقليدية أو السيرية بسهولة وأقل كلفة مقابل صعوبة اكتشاف حقيقة المحتوى المزيف واكتشاف المجرم.
- قصور القوانين السيرية في مواجهة كافة أشكال جرائم التزييف العميق وخلوها من الإجراءات الوقائية والعلاجية لهذا النوع من الجرائم.
- أهمية وجود أدوات المكافحة الثلاثية القانونية والتكنولوجية والخاصة والإعلامية للتصدي لهذا النوع من الجرائم.

112 I. Gangji, Tackling Deepfakes in Journalism, International Center for Journalists (2022). <https://www.icfj.org/news/tackling-deepfakes-journalis> (last visited Aug 25, 2023).

113 Vizoso, Vaz-Álvarez & López-García, supra note 22, p. 296.

### ثانيًا: التوصيات

- يجب على المشرع الوطني تبني سياسات وإجراءات تضمن اشتغال تطبيقات التزييف العميق على المعلومات الكافية حول كيفية الاستخدام الإيجابي، وبيان المخاطر التي تترتب على الاستخدام السلبي.
- إصدار تشريع خاص بالتزييف العميق يتناول أنواع الجرائم وعقوبة كل منها، وقيمة التعويض عن الأضرار التي تترتب على كل جريمة.
- إلزام الشركات المحلية المنتجة والمشغلة لهذه التكنولوجيا، وكذلك مزودو الخدمة بتبني إجراءات تمنع وتكافح سوء الاستخدام كتبني تكنولوجيا العلامة المائية الذكية، والتحقق من هوية المستخدم، وتشكيل وحدات خاصة تقوم بمراقبة وإزالة المحتوى المزيف.
- إنشاء وحدات خاصة لدى أجهزة الأمن كي تتعامل بسرعة مع شكاوى الأشخاص الطبيعيين والاعتباريين المستهدفين بتقنية التزييف العميق.

## المراجع

أولاً: العربية

1 - كتب ومقالات:

أبو عفيفة، طلال. أصول علمي الإجرام والعقاب وآخر الجهود الدولية والعربية لمكافحة الجريمة المنظمة عبر الحدود الوطنية. دار الجندي للنشر والتوزيع، القدس، 2013.

الحسن، عبد العزيز أحمد. شرح قانون الجرائم والعقوبات الاتحادي لدولة الإمارات العربية المتحدة الصادر بموجب المرسوم بقانون اتحادي رقم 31 لسنة 2021: الأحكام العامة - الكتاب الأول - النظرية العامة للجريمة. دار النهضة العلمية، دبي، القاهرة، 2022.

زكير، أحمد عبد الموجود. «جريمة التزييف الإباحي العميق: دراسة مقارنة». المجلة القانونية، كلية الحقوق (فرع الخرطوم)، جامعة القاهرة، مج 11، ع 7، 2022.

2 - قوانين:

قانون الجرائم الإلكترونية الأردني لسنة 2023.

قانون مكافحة الشائعات والجرائم الإلكترونية الإماراتي رقم (34) لسنة 2021:

قانون مكافحة الجرائم الإلكترونية القطري رقم (14) لسنة 2014:

ثانياً:

## References

## 1- Books:

Abu Afifa, Talal. *Usul Ilmi al-Ijraam wa al-'Iqab wa Akhir al-Juhud al-Dawliyah wa al-Arabiyah li Mukaafahat al-Jirmah al-Munazzamah 'Abr al-Hudud al-Wataniyah*. (in Arabic), Dar al-Jundi lil Nashr wa al-Tawzee', al-Quds.

Al-Hasan, Abdul Aziz Ahmed. *Sharh Qanoon al-Jara'im wa al-'Iqabat al-Ittihad li Dawlat al-Imarat al-Arabiyah al-Muttahidah: al-Ahakam al-'Amah - al-Kitab al-Awwal*, (al-Nazariyah al-'Amah lil Jirmah) (in Arabic), Dar al-Nahdah al-'Ilmiyah, 2022.

Pic, M., et al. Face Manipulation Detection in Remote Operational System, in C. Rathgeb et al. (Eds.), *Handbook of Digital Face Manipulation and Detection: From DeepFakes to Morphing Attacks* 431 (Springer 2022).

Tolosana, R., et al. "Future Trends in Digital Face Manipulation and Detection," in C. Rathgeb et al. (Eds.), *Handbook of Digital Face Manipulation and Detection: From DeepFakes to Morphing Attacks* 463 (Springer 2022).

Tolosana, R., et al. "An Introduction to Digital Face Manipulation," in C. Rathgeb et al. (Eds.), *Handbook of Digital Face Manipulation and Detection: From DeepFakes to Morphing Attacks 4* (Springer 2022).

Zakīr, Aḥmad ‘Abd al-Mawjūd. "Jirīmah al-tazwīf al-ibāhī al-‘amīq: dirāsah muqāranah," (in Arabic), *al-Majallah al-qānūniyah*, Jāmi‘at al-Qāhirah, Kullīyat al-ḥuqūq (Fir‘ al-Khartūm), Vol. 11, No. 7, 2022.

## 2- Journals:

Barber, A. Freedom of Expression Meets Deepfakes, 202 *Synthese* 40 (2023). <https://doi.org/10.1007/s11229-023-042664>.

Bothamley, S., & Tully, Ruth J. Understanding Revenge Pornography: Public Perceptions of Revenge Pornography and Victim Blaming, *Journal of Aggression, Conflict and Peace Research* (2018), doi: 10.1108/JACPR-09-2016-0253.

Chesney, B., & Citron, D. Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security, 107 *California Law Review* 1753 (2019).

Dixon, H. Deepfakes: More Frightening Than Photoshop on Steroids, 58 *Judges Journal* 36 (2019).

Dobber, T., et al. Do (Microtargeted) Deepfake Have Real Effects on Political Attitudes? 26 *The International Journal of Press/Politics* 72 (2021).

Ellamey, M, Y., "Criminal Protection from disinformation during electoral campaigns in light of the legislative Criminal Policy – A Comparative Study with Egyptian and French Legislations" (in Arabic) *International Review of Law*, Volume 9, Issue 3, 2020 Special Issue on the conference of "Law and Media: Horizons and Challenges".

Farid, H. Deepfakes: A Looming Challenge for Privacy, Democracy, and National Security, 134 *Harvard Law Review* 1755 (2020).

Hancock, TJ. & Bailenson, NJ. The Social Impact of Deepfakes, 24 *Cyberpsychology, Behaviour, and Social Networking* 149 (2021).

Harris, J. Deepfake Detection: A Comprehensive Review, 19 *Journal of Computer Science* 345 (2021).

Luochen, L. Smart Watermark to Defend against Deepfake Image Manipulation, in 2021 IEEE 6<sup>th</sup> International Conference on Computer and Communication Systems 380 (2021).

Martinez, A. Deepfakes and the Law: A Legal Perspective, 130 *Yale Law Journal* 1020 (2021).

Taylor, L. Deepfakes and Gender: A Feminist Perspective, 29 *Gender Studies Quarterly* 210 (2021). <https://gsq.org/deepfakes-and-gender>.

Vizoso, A., Vaz-Álvarez, M., & López-García, X. Fighting Deepfakes: Media and Internet Giants’ Converging and Diverging Strategies Against Hi-Tech Misinformation, 9 *Media and Communication* 291 (2021).

Wahl-Jorgensen, K., & Carlson, M. Conjecturing Fearful Futures: Journalistic Discourses on Deep-fakes, 15 *Journalism Practice* 803 (2021). <https://doi.org/10.1080/17512786.2021.1908838>.

Zhang, J. AI-Deep Synthesis Regulations and Legal Challenges: Recent Face Swap Fraud Cases in China. *Lexology*. <https://www.lexology.com/library/detail.aspx?g=1a3455cc-dc4d-4ed0-918a-c3429999c31f>.

### Reports:

Brooks, T., et al. "Increasing Threat of Deepfake Identities," Department of Homeland Security, USA (2023). [https://www.dhs.gov/sites/default/files/publications/increasing\\_threats\\_of\\_deepfake\\_identities\\_0.pdf](https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf).

Daniel L., et al. "Deepfakes and International Conflict," The Brookings Institution, Washington DC, P3 (2023).

Engler, A. "Fighting Deepfakes When Detection Fails," Brookings Institution (2019). <https://policy-commons.net/artifacts/4139532/fighting-deepfakes-when-detection-fails/4947455>) last visited July(2023 ,28 .

Goodfellow, IJ., et al. "Generative Adversarial Nets," *NeurIPS*, [https://proceedings.neurips.cc/paper\\_files/paper/2014/file/5ca3e9b122f61f8f06494c97b1afccf3-Paper.pdf](https://proceedings.neurips.cc/paper_files/paper/2014/file/5ca3e9b122f61f8f06494c97b1afccf3-Paper.pdf). f (last visited June 5, 2023).

Huijstee, M., et al. "Tackling Deepfakes in European Policy," European Parliamentary Research Service (2021). [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS\\_STU\(2021\)690039\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf) (last visited Jun 14, 2023)

Harrison, K. Leopold, A., et al. "The State of Deepfake," *Deeprust Alliance* (2020). <https://static1.square-space.com/static/5d894b6dcd6a2255c38759fe/t/6046e099e1c70c281fe57447/1615257771315/Pornographic+Deepfake+Report+Part+1.pdf> (last visited July 11, 2023).

Li, Y., & Lyu, S. "Exposing DeepFake Videos by Detecting Face Warping Artifacts," Cornell University (2018). <https://arxiv.org/pdf/1811.00656.pdf> (last visited May 24, 2023).

Madiega, T. *Artificial Intelligence Act*, EPRS | European Parliamentary Research Service (2023).

Petkauskas, V. "Report: Number of Expert-Crafted Video Deepfakes Double Every Six Months," *CyberNews* (2021). <https://cybernews.com/privacy/report-number-of-expert-crafted-video-deep-fakes-double-every-six-months> (last visited 09/07/2023).

Rosenthal, L., et al. "The Content Authenticity Initiative: Setting the Standard for Digital Content Attribution," *CAI* (2020).

Sheehan, M. "China's AI Regulations and How They Get Made," Carnegie Endowment for International Peace (2023), Carnegie Endowment for International Peace, Publications Department, 1779 Massachusetts Avenue NW.

Wittes, B., et al. "Sextortion: Cybersecurity, Teenagers, and Remote Sexual Assault," Brookings Institution (2016). <https://www.brookings.edu/wp-content/uploads/2016/05/sextortion1-1.pdf> (last visited June 7, 2023).

### 3- Legislation:

China Provisions on the Administration of Deep Synthesis Internet Information Services.

Criminal Law of the People's Republic of China 1997.

DEEP FAKES Accountability Act 2020.

### 4- Internet Sources:

Ayyub, R. "I Was the Victim of a Deepfake Porn Plot Intended to Silence Me," HuffPost UK News (2018). [https://www.huffingtonpost.co.uk/entry/deepfake-porn\\_uk\\_5bf2c126e4b0f32bd58ba316](https://www.huffingtonpost.co.uk/entry/deepfake-porn_uk_5bf2c126e4b0f32bd58ba316) (last visited June 6, 2023).

Bartz, D. "Microsoft Chief Says Deep Fakes are Biggest AI Concern," Reuters (2023). <https://www.reuters.com/technology/microsoft-chief-calls-humans-rule-ai-safeguard-critical-infrastructure-2023-05-25> (last visited July 16, 2023).

Beckerman, R., et al. "Adobe, The New York Times Company and Twitter Announce Content Authenticity Initiative to Develop Industry Standard for Content Attribution," Adobe News (2019). <https://news.adobe.com/news./news-details/2019/Adobe-The-New-York-Times-Company-and-Twitter-Announce-Content-Authenticity-Initiative-to-Develop-Industry-Standard-for-Content-Attribution/default.aspx>(last visited July 20, 2023).

Bienkov, A. "Boris Johnson Appeared to Endorse Jeremy Corbyn for Prime Minister in a Convincing Deepfake Video," Business Insider (2019). <https://www.businessinsider.com/video-boris-johnson-endorse-jeremy-corbyn-in-convincing-deepfake-2019-11> (last visited July 14, 2023).

Burt, J. "Deepfakes Being Used in 'Sextortion' Scams, FBI Warns," The Register (2023). [https://www.theregister.com/2023/06/08/ai\\_deepfakes\\_sextortion\\_fbi](https://www.theregister.com/2023/06/08/ai_deepfakes_sextortion_fbi) (last visited June 9, 2023).

Chickowski, E. "Criminals Use Deepfake Videos to Interview for Remote Work," Dark Reading (2022). <https://www.darkreading.com/attacks-breaches/criminals-deepfake-video-interview-remote-work> (last Visited August 22, 2023).

China Law Translate. "Provisions on the Administration of Deep Synthesis Internet Information Services." <https://www.chinalawtranslate.com/en/deep-synthesis> (last visited August 24, 2023).

- Chun Ki Chan, C., et al. "Combating Deepfakes: Multi-LSTM and Blockchain as Proof of Authenticity for Digital Media," IEEE/ITU (2020). <https://ieeexplore.ieee.org/abstract/document/9311067> (last visited July 17, 2023).
- Colaner, N., & Quinn, M.J. Deepfakes and the Value-Neutrality Thesis (2020). <https://www.seattleu.edu/ethics-and-technology/viewpoints/deepfakes-and-the-value-neutrality-thesis.html> (last visited May 27, 2023).
- Cook, J. "Deepfake Technology: Assessing Security Risk," School of Informational Service, American University (2022). [https://www.american.edu/sis/centers/security-technology/deepfake\\_technology\\_assessing\\_security\\_risk.cfm](https://www.american.edu/sis/centers/security-technology/deepfake_technology_assessing_security_risk.cfm) (last visited August 19, 2023).
- Damiani, J. "A Voice Deepfake Was Used to Scam A CEO Out Of \$243,000," Forbes (2019). <https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/> (last visited June 7, 2023).
- Dickson, E. "AI Deepfakes of True-Crime Victims Are a Waking Nightmare," Rolling Stone (May 30, 2023). <https://www.rollingstone.com/culture/culture-features/true-crime-tiktok-ai-deepfake-victims-children-1234743895> last visited Aug.(2023 ,22
- Feiner, L. "Facebook Says the Doctored Nancy Pelosi Video Used to Question her Mental State and Viewed Millions of Times Will Stay up," CNBC News (2019). <https://www.cnbc.com/2019/05/24/fake-nancy-pelosi-video-remains-on-facebook-and-twitter.htm> (last visited March 7, 2023)
- Fowler, G. "Anyone with an iPhone Can Now Make Deepfakes. We Aren't Ready for What Happens Next," The Washington Post (2021). <https://www.washingtonpost.com/technology/2021/03/25/deepfake-video-apps/> (last visited Jun 01, 2023).
- Gangji, I. "Tackling Deepfakes in Journalism," International Center for Journalists (2022). <https://www.icfj.org/news/tackling-deepfakes-journalis> (last visited Aug 25, 2023).
- Hao, K., & Heaven, W. D. "The year deepfakes went mainstream," MIT Technology Review (2020).
- International Telecommunication Union, "Deepfake Technology: Global Standards and Guidelines." <https://www.itu.int/deepfake-technology-global-standards> (last visited May 27, 2023).
- Johnson, R. "Deepfakes in Healthcare: Opportunities and Risks," Medical News Today (2022). <https://www.medicalnewstoday.com/deepfakes-in-healthcare>.
- Kropotov, V., et al. "How Underground Groups Use Stolen Identities and Deepfakes," Trend Micro (2022). [https://www.trendmicro.com/en\\_us/research/22/i/how-underground-groups-use-stolen-identities-and-deepfakes.html](https://www.trendmicro.com/en_us/research/22/i/how-underground-groups-use-stolen-identities-and-deepfakes.html) (last visited Aug 22, 2023).

- Laje, D., "China's Deep Fake Law Is Fake," (2023). <https://www.afcea.org/signal-media/cyber-edge/chinas-deep-fake-law-fake> (last visited Aug 24, 2023).
- Lenthang, M. "Cheerleader's Mom Created Deepfake Videos to Allegedly Harass her Daughter's Rivals," ABC News (2021). <https://abcnews.go.com/US/cheerleaders-mom-created-deepfake-videos-allegedly-harass-daughters/story?id=7643759> (last visited 26 May, 2023).
- Mariyam B. "EcoChamp Reviews: Is EcoChamp Com Legit or Scam?" Zero Thought (2023). <https://zerothought.in/ecochamp-reviews-july-2022-is-ecochamp-com-my-legit-or-scam> (last visited 26 May 2023).
- Novak, M. "Elon Musk Impersonator Scams Promise Free Neuralink Brain Chip in Paid Ads on Twitter," Forbes (2023). <https://www.forbes.com/sites/digital-assets/2023/02/28/elon-musk-crypto-scams-promise-free-neuralink-brain-chip-in-paid-ads-on-twitter/?sh=75abe6d47b4f> (last visited June 7, 2023).
- Pantserev, K.A., The Malicious Use of AI-Based Deepfake Technology as the New Threat to Psychological Security and Political Stability. In: H. Jahankhani, et al. (ed.) Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity. Advanced Sciences and Technologies for Security Applications. Springer, Cham (2020). [https://doi.org/10.1007/978-3-030-35746-7\\_3](https://doi.org/10.1007/978-3-030-35746-7_3) (last visited Jun 5, 2023).
- Rees, G. "Here's how Deepfake Technology can Actually be a Good Thing," World Economic Forum (2019). <https://www.weforum.org/agenda/2019/11/advantages-of-artificial-intelligence> (last visited August 19, 2023).
- Rehan, A. "12 AI Voice Cloning Tools to Create Seamless Authentic Voiceovers," Geekflare (2023). <https://geekflare.com/aivoicecloningtools/?s=12+AI+Voice+Cloning+Tools+to+Create+Seamless+Authentic+Voiceovers> (last visited Aug 09, 2023).
- Roose, K. "Here come the Fake Videos, Too," The New York Times (2018). <https://www.nytimes.com/2018/03/04/technology/fake-videos-deepfakes.html> (last visited June 5, 2023).
- Shivangi, A. "15 Best Deepfake Apps & Websites that You Must Try," Smartprix (2023). <https://www.smartprix.com/bytes/14-best-deepfake-apps-websites-for-entertainment> (last visited Aug 09, 2023).
- Ulmer, A., & Tong, A. "Deepfaking it: America's 2024 election collides with AI boom," Reuters (2023). <https://www.reuters.com/world/us/deepfaking-it-americas-2024-election-collides-with-ai-boom-2023-05-30> (last visited July 14, 2023).
- Vaccari, C and Andrew Chadwick, Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News, *Social Media + Society*, 6(1).

- Vincent, J. "Why we need a better definition of 'deepfake,'" The Verge (2018). <https://www.theverge.com/2018/5/22/17380306/deepfake-definition-ai-manipulation-fake-news> (last visited Jun 3, 2023).
- Wiggers, K. "Facebook, Microsoft and Others Launch Deepfake Detection Challenge," VentureBeat. <https://venturebeat.com/ai/facebook-microsoft-and-others-launch-deepfake-detection-challenge> (last visited Aug 25, 2023).
- Wong, R. "Stop Screening Job Candidates' Social-Media," Harvard Business Review (2021). <https://hbr.org/2021/09/stop-screening-job-candidates-social-media> (last visited June 10, 2023).