

المواجهة الجنائية لتقنية الديق فيك (Deep fakes)

من إعداد

د . أشرف سيد أبو العلا

دكتوراه القانون الجنائي

كلية الحقوق - جامعة أسيوط

ملخص البحث

يشير مصطلح التزييف العميق الذي ظهر لأول مرة في عام ٢٠١٧، إلى استخدام برنامج الذكاء الاصطناعي (AI) للتلاعب في محتوى الصوت والفيديو، وتتيح هذه التقنية إمكانية إنشاء مقاطع فيديو مزيفة عن طريق التلاعب بالصور والأصوات باستخدام تقنية التعلم العميق، لذا فقد سميت التزييف العميق أو التعديل الذكي للوجوه وتسمى أيضا مقاطع الفيديو المزيفة أو مقاطع الفيديو عميقة التزوير . والهدف من مقاطع الفيديو هذه هو جعل أي شخص يفعل أو يقول أي شيء لأي شخص^(١)، ويسهل الوصول إلى هذه التقنية نسبيا، فبعض برامج التعلم العميق المخصصة لمقاطع الفيديو أو الصور شديدة التلاعب موجودة على الويب في مصدر مفتوح أي خالية من الحقوق، وفي المقابل فإن مواجهتها ليست بهذه السهولة.

وبذلك يعد الذكاء الاصطناعي تكنولوجيا جديدة، ليس فقط على المستوى القانوني، ولكن على جميع المستويات، ولذلك ازداد الخوف والقلق من الأضرار التي تسببها تطبيقات الذكاء الاصطناعي إذا خرجت عن سيطرة المنتجين لها وتم تشغيلها واستخدامها في الإضرار بالغير كما هو الحال في تقنيات الديق فيك (التزييف العميق).

وفي ذلك إعلان صريح عن دخول الجريمة عصرا يستوجب تحركا فقهيا وتشريعا وقضائيا بما يواكب معطيات العصر الحديث^(٢)، وهو ما سنقوم ببيانه باستخدام المنهج الوصفي التحليلي من خلال المباحث التالية:

المبحث الأول: ماهية تقنية الديق فيك (Deep fakes) وخصائصها.

المبحث الثاني: مخاطر تقنية الديق فيك (Deep fakes) وتطورها.

المبحث الثالث: المواجهة التشريعية لمخاطر تقنية الديق فيك (Deep fakes).

(١) Claire Langlais-Fontaine, Démêler le vrai du faux: étude de la capacité du droit actuel à lutter contre les deepfakes, La Revue des droits de l'homme, N°١٨, ٢٠٢٠, p.١٠.

(٢) د. محمد شوقي العناني، د. إسلام هديب، الذكاء الاصطناعي ودوره في مكافحة الفساد، دار النهضة العربية، القاهرة، ٢٠٢٢م، ص ٥٤.

Abstract

The term deepfakes, which first appeared in ٢٠١٧, refers to the use of artificial intelligence (AI) software to manipulate audio and video content. This technology allows the creation of fake videos by manipulating images and sounds using deep learning technology. Smart face editing is also called fake videos or deepfakes. The goal of these videos is to make anyone do or say anything to anyone, and this technology is relatively easy to access, as some deep learning programs dedicated to highly manipulated videos or images are on the web in open source, On the other hand, confronting them is not so easy.

Thus, artificial intelligence is a new technology, not only at the legal level, but at all levels. Therefore, fear and anxiety about the damage caused by artificial intelligence applications increased if they got out of the control of their producers and were operated and used to harm others, as is the case in Deep Fake technologies.

And in that is an explicit declaration that the crime has entered an era that requires jurisprudence, legislative and judicial action in keeping with the data of the modern era, which we will explain using Analytical descriptive approach through the following investigations:

The first topic What is deepfake technology and its characteristics.

The second topic: Risks and development of deepfake technology.

The third topic: Legislative confrontation of the dangers of Deepfake technology.

مقدمة

أولاً: موضوع البحث:

تعتبر تقنية الـديب فيك (Deep fake) واحدة من أكثر التطورات التكنولوجية تقدماً وخطورة في عالم التلاعب بالوسائط المتعددة، حيث إنها تستخدم الذكاء الاصطناعي وتقنيات التعلم العميق لإنتاج مقاطع فيديو أو صوتية تبدو وكأنها حقيقية، ولكنها في الواقع مزيفة بشكل مميز، وتمثل هذه التقنية تحدياً كبيراً للمجتمع القانوني والأمان السيبراني، وتثير مخاطر جنائية متعددة يجب مواجهتها بشكل جدي.

وتعمل البرامج المستخدمة في التزييف العميق عن طريق آلية محددة قادرة على خداع خوارزميات الاكتشاف وبناء على المنافسة بين خوارزميتين: تقوم الأولى بنسخ مقطع فيديو متطابق عدة مرات عن طريق استيراد وجه خارجي إليه، وتكشف الثانية جودة مقاطع الفيديو التي تم إنشاؤها بواسطة الخوارزمية الأولى من أجل استبعاد الأقل مصداقية، وهو ما يطلق عليه تقنية "GAN"، أي شبكات الخصومة التوليدية التي تهدف إلى التدريب على إنشاء محتوى مزيف يشبه المحتوى الأصلي، بحيث تصعب التفرقة بينهما، سواء عن طريق العين البشرية أو الأجهزة الآلية، وبالتالي، فإن تقنية التزييف العميق تهدف إلى إنشاء مقاطع فيديو واقعية للغاية مع توفير الحماية من الكشف السريع عن المنتج المزيف^(١).

ويتيح التزييف الإباحي العميق إمكانية استيراد وجوه الأفراد، سواء العاديين أم مشاهير السياسة والفن إلى أجسام الأشخاص الذين يؤديون الأدوار في الفيديوهات الإباحية، ثم نشر هذه الفيديوهات، دون موافقة الضحايا على هذا النشر.

وبالرغم من الانتشار الملحوظ للإساءة القائمة على الصور، ومنها التزييف الإباحي العميق، إلا أن تحديد حجم هذه الظاهرة على وجه الدقة من الأمور التي تواجه صعوبة نظراً لعدم كثرة البيانات التي تم جمعها بشكل منهجي في الدراسات التي تناولتها، وغالباً يتم الإبلاغ عن التعرض لهذا النوع من الإيذاء من قبل المجني عليهم، وكثير من هؤلاء يكون على غير دراية بما قام به الجاني من إساءة استخدام الصورة دون إذنه، يضاف إلى ذلك عدم الاتفاق بين الجهات الفاعلة والتشريعات المختلفة حول طبيعة الصور التي تكون محلاً لهذا السلوك والعناصر الأخرى الواجب توافره لقيام مسؤولية الجاني، ومن ذلك على سبيل المثال في حالة التآزر الإباحي، لا يوجد اتفاق حول مدى وجوب أن تكون الصور المعنية صوراً جنسية صريحة، وكذلك الأمر في شأن مدى وجوب توافر القصد الخاص لدى الجاني^(٢).

وبالرغم مما تقدم فإنه يمكن الاستشهاد ببعض البيانات من مصادر مختلفة للقول بأن النسبة التي

(١) Claire Langlais-Fontaine, Démêler le vrai du faux: étude de la capacité du droit actuel à lutter contre les deepfakes, La Revue des droits de l'homme, N°١٨ | ٢٠٢٠. p.١.

(٢) bid.

تستهويها هذه السلوكيات ليست قليلة، ومن ذلك ما أدلى به مؤسس احد المواقع المتخصصة في استضافة الصور لغرض الانتقام الإباحي، حيث صمم Hunter Moore موقعا باسم IsAnyoneUp عام ٢٠١٠ لمشاركة صورة عارية لشريكته مع أصدقائه، وبعد أسبوع واحد من إنشاء الموقع تفاجئ بوجود أكثر من ١٤٠٠٠ زائر للموقع، وظل هذا الموقع نشطا لمدة ستة عشر شهرا استقبل خلالها مؤسسه في كل أسبوع منها حوالي ٣٥٠٠٠ صورة إباحية نصفها تم تقديمه ذاتيا بهدف الشهرة السريعة على الإنترنت والنصف الآخر كان مزودا بالاسم الكامل للضحية ومهنتها ومحل إقامتها لغرض الانتقام منها^(١).

وتكشف حالات الإبلاغ المعلن عنها في بعض الدول فور تجريمها هذا السلوك عن أن عددا غير قليل من الأفراد قد تعرضوا له، ففي إنجلترا وويلز على سبيل المثال تم تجريم هذا السلوك في أبريل ٢٠١٥، وشهدت الستة أشهر التالية للعمل بالقانون ١١٦٠ حادثة تم الإبلاغ عنها بالفعل، وكان متوسط عمر الضحايا في هذه الوقائع ٢٥ عاما، وبعضهم لم يبلغ الحادية عشر من عمره، وكان موقع التواصل الاجتماعي Facebook هو الأكثر استخداما كمسرح الجريمة، حيث تم استخدامه في ارتكاب ٦٨% من الجرائم التي تم الإبلاغ عنها^(٢)، فإذا أخذ في الاعتبار أن العدد المشار إليه هو عدد الحالات التي تم الإبلاغ عنها بالفعل خلال ستة أشهر فقط من التجريم، وأن كثيرا من الضحايا لا يتقدمون ببلاغات مشابهة، سواء لتنازلهم عن حقهم في مقاضاة الجاني، أم لعدم درايتهم بكونهم ضحايا، فإن ذلك يكشف عن تنامي ظاهرة الإيذاء القائمة على الصور بشكل يستوجب التصدي لها بالعقوبات الجنائية الملائمة، وتؤكد هذه الزيادة دراسة استقصائية أجريت في استراليا عام ٢٠١٧ شملت ٤٢٠٠ مشاركا، حيث كشفت هذه الدراسة عن أن نسبة ٢٠% من المشاركين قد تعرضت للإساءة القائمة على الصور وكان الباحثون أنفسهم قد أجروا مسحا في عام ٢٠١٤ وكانت نسبة من لهم تجربة مع هذا السلوك تقف عند ١٠.٧%، وهو ما يعني أن هذه النسبة تضاعفت خلال ثلاث سنوات فقط، مما يشير بوضوح إلى زيادة سريعة في معدلات هذا النوع من الإيذاء^(٣) كما أشارت هذه الدراسة إلى أن أكثر من ٩٠% من الضحايا هم من الشركاء السابقين أو المعروفين للجاني، كما أشارت إلى أن ٥٤% من الجناة كانوا من الذكور، و ٣٣% من الإناث، و ١٣% إما غير معروفين أو يمثلون مجموعة مختلطة من الذكور والإناث^(٤).

(١) Scott R. Stroud, The Dark Side of the Online Self: A Pragmatist Critique of the Growing Plague of Revenge Porn, Journal of Mass Media Ethics, ٢٩(٣), ٢٠١٤, pp. ١٦٨-١٨٣, p. ١٧٠.

(٢) Majid Yar, Jacqueline Drew, Image-Based Abuse, Non-Consensual Pornography, Revenge Porn: A Study of Criminalization and Crime Prevention in Australia and England & Wales, International Journal of Cyber Criminology, Vol ١٣ Issue ٢ July - Dec. ٢٠١٩, p. ٥٨٢.

(٣) Nicola Henry, Anastasia Powell & Asher Flynn: Not Just 'Revenge Pornography': Australians' Experiences of Image-Based Abuse, RMIT University, may ٢٠١٧, p. ٥

(٤) Ibid.

ووفقا لتقرير أصدرته شركة Deep Trace ، وهي شركة هولندية تعمل في أنظمة الحوسبة وتهتم بدراسة التزييف العميق، تم تحميل ١٤٠٠٠ مقطع فيديو شديد التلاعب في عام ٢٠١٩ ، وهو ما يمثل زيادة بنسبة ٨٤% عن العام السابق. تم التعرف على أكثر من ٨٥٠ شخصا كضحايا لمقاطع الفيديو شديدة التلاعب، وكانت نسبة ٩٦% من مقاطع الفيديو المزيفة هي مقاطع فيديو إباحية^(١). وقد نمت هذه الظاهرة إلى حد أنه تم إنشاء منصات مخصصة لمقاطع الفيديو التي أنشئت بتقنية التزييف العميق، مما يدل على وجود سوق لمواقع الويب التي تستضيف هذا النوع من مقاطع الفيديو، وهو ما يوجب ضرورة التصدي لهذه الممارسات.

ثانيا: أهمية البحث:

ليس هناك شك أن ثمة ضرورة لملاحقة التشريع الجنائي للمستجدات الحديثة والتي تمثل خطرا على المصالح الجوهرية الجديرة بالحماية في جميع المجتمعات، وعلى الأخص في العصر الحديث الذي تتسارع فيه أوجه التكنولوجيا نحو ابتكار العديد من التقنيات الحديثة التي تثير بقدر أهميتها وأحيانا ضرورتها مخاوف وشكوك كثيرة.

واحدة من هذه التقنيات هي تقنية التزييف العميق (Deep fakes) التي يمكن من خلالها اصطناع مقاطع فيديو لأشخاص ما يصعب وربما يستحيل أحيانا اكتشاف تزييفها كذلك صور وتسجيلات صوتية^(٢)، تلك الجرائم التي صنفت ضمن الأخطر في مجال الذكاء الاصطناعي، وتعتمد تلك التقنية الحديثة على التعلم العميق (Deep Learning) والتعلم الآلي (Machine Learning) كأداتين لفحص تعابير الوجه وحركات الشخص المراد تزييفه مثل الابتسامة ونظرة العين والإيماء وحركة الشفاه، وتجميع صوراً لوجه ونبرات الصوت، ثم بعد ذلك يتم تغذية التطبيق بها لتنتج لنا مقاطع فيديو مماثلة للتعبيرات والحركات بشكل طبيعي مسجلة لشخصيات عامة يتكلمون، تبدو واقعية للغاية، مع أنهم في الحقيقة لم ينطقوا بكلمة واحدة مما جاء فيها^(٣).

وبذلك تكمن أهمية البحث في المعالجة الجنائية للحد من مخاطر تلك الظاهرة المستحدثة والتي تمكن الأفراد من التشهير والإساءة بالغير من خلال نشر مقاطع فيديو مفبركة يصعب اكتشاف تزييفها، تمثل انتهاكا للحق في الشرف والاعتبار من ناحية، والحق في الخصوصية من ناحية أخرى، بالإضافة إلى سلبيات إهدار حجية الأدلة الرقمية أمام الجهات القضائية نظرا لما يعترى تلك الأدلة من شبهات.

(١) Rapport: The State Of Deepfakes, Landscape, Threats and Impact, Deeprtrace, ٢٧ septembre ٢٠١٩, PP. ١-٣

(٢) Elena Igorevna Galyashina, Vladimir Dmitrievich Nikishin, The protection of megascience projects from deepfake technologies threats: information law aspects, Journal of Physics: Conference Series, ٢٠٢٢, p. ٥.

(٣) Robert Chesney, and Danielle Citron, Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. Foreign Affairs, ٢٠١٩, ٩٨, ١٤٧.

ثالثاً: إشكالية البحث وتساؤلاته:

لما كان التزييف الإباحي العميق يقع على صورة المجني عليه، والحصول على هذه الصورة قد يتم بموافقة من تمثله، وقد تكون متاحة على الإنترنت أو التقطها الجاني في مكان عام، فإن مشكلة البحث تدور حول مدى مشروعية التزييف الإباحي العميق إذا كان الجاني قد حصل على الصورة قبل تزييفها بطريق مشروع، وكذلك مدى مشروعية نشر الصورة بعد تزييفها إذا كانت قد خضعت لتقنية التزييف العميق بموافقة من تمثله.

وبذلك تتمثل المشكلة الرئيسية في هذا التساؤل المطروح على بساط البحث:

- ١ - ماهية تقنية الديب فيك.
- ٢ - ماهي خصائص تقنية الديب فيك.
- ٣ - ما هي مخاطر تقنية الديب فيك.
- ٤ - كيف نشأت وتطورت تقنية الديب فيك.
- ٥ - كيفية مواجهة التشريعية لمخاطر تقنية الديب فيك.

خامساً: أهداف البحث:

من خلال عرض إشكالية وتساؤلات البحث فإن أهداف البحث الرئيسية تتمثل في التعرف على:

- ١ - ماهية تقنية الديب فيك.
- ٢ - خصائص تقنية الديب فيك.
- ٣ - مخاطر تقنية الديب فيك.
- ٤ - نشأت وتطور تقنية الديب فيك.
- ٥ - المواجهة التشريعية لمخاطر تقنية الديب فيك.

سادساً: منهجية البحث:

وفى سبيل تحقيق الدراسة لأهدافها، فقد استخدمت المنهج الوصفي التحليلي، من خلال وصف هذه الظاهرة الإجرامية، وتحليلها في ضوء التشريعات والقوانين وأراء الفقه للخروج بالنتائج والتوصيات التي يمكن من خلالها مواجهة تلك الظاهرة الإجرامية حماية لحق الضحايا في الخصوصية والكرامة الإنسانية من ناحية، وتحقيق الأمن والاستقرار الاجتماعي من ناحية أخرى.

المبحث الأول

ماهية تقنية الـديب فيك (Deep fakes) وخصائصها

تمهيد وتقسيم:

تعتمد تقنية الـديب فيك (Deep fake) على استخدام الذكاء الاصطناعي لإنشاء محتوى مزيف أو مزيف بصري وصوتي يبدو وكأنه حقيقي، وتعتمد تلك التقنية على الشبكات العصبية العميقة (Deep Neural Networks) لتوليد هذا المحتوى الزائف، والذي يمكن أن يشمل فيديوهات، صور، أصوات، وحتى نصوص.

مما جعل استخدام تقنية الـديب فيك يثير قلقاً كبيراً بشأن الاستخدامات السلبية مثل الاحتيال والتلاعب السياسي والاستهلاك الإعلامي الخاطيء، كما يمكن استخدامها لخداع الجمهور ونشر معلومات زائفة. وبذلك فهناك تحديات أمنية وقانونية مرتبطة بتقنية الـديب فيك، بما في ذلك استخدامها في الاحتيال والتجسس، وهذا يعني أنه يجب وضع إطار قانوني مناسب لمنع سوء الاستخدام. ولكن قبل وضع ذلك الإطار القانوني كان لزاماً علينا التعرف لماهية تقنية الـديب فيك (Deep fakes) وخصائصها، وذلك من خلال المطالبين التاليين:

المطلب الأول: ماهية تقنية الـديب فيك (Deep fakes).

المطلب الثاني: خصائص تقنية الـديب فيك (Deep fakes).

المطلب الأول

ماهية تقنية الـديب فيك

تعرف تقنية الـديب فيك أو التزييف العميق deep fake بأنها التقنية التي يمكن من خلالها عمل مقاطع فيديو مزيفة لأشخاص يصعب إن لم يكن من المستحيل كشفها، على الأقل بالنسبة للأشخاص العاديين^(١)، وأنها معالجة صور للأشخاص وتحويلها إلى مقاطع فيديو باستخدام برامج كمبيوتر معينة، لتحول هؤلاء الأفراد إلى مشاركين في أفعال لم يساهموا في ارتكابها^(٢).

ويعرف الـديب فيك (التزييف العميق) أيضا بأنه عملية تصنيع صور أو اختلاقتها باستخدام شبكات الذكاء الاصطناعي، والذي غالبا ما يكون باستخدام وجه أو صوت أحد الأفراد بقصد عمل فيديو أو تسجيل صوتي مشابه للفرد الذي يتم عمل التزييف العميق للفيديو أو التسجيل الصوتي له^(٣).

وتعد هذه التقنية أشد خطورة من خطورة برنامج الفوتوشوب، الذي كان يستخدم في تزييف الصور، وقد تم استخدام هذه التقنية في التلاعب في الانتخابات والأمن القومي، غير ذلك من الأفعال التي تستخدمها الأجهزة الاستخباراتية في تفويض الثقة في المؤسسات العامة في الدولة^(٤).

إلا أن عمل الـديب فيك باستخدام لوغاريتمات لا يعني أن الأمر أصبح من المسلمات الواقعية التي لا حل لها من الناحية التقنية، فإذا كانت هذه التقنية تتم عن طريق لوغاريتم، فلا شك أنه يمكن الوصول للوغاريتم آخر يساهم في كشفها، غير أن الأمر ليس على هذه الدرجة من السهولة من الناحية التقنية، وإنما عملية استخدام تقنيات الـديب فيك في تطور مستمر.

وحول التعريف القانوني لتقنية التزييف العميق (الديب فيك)، فهناك الكثير من التشريعات التي لم تضع تعريف جامع مانع للتقنية الـديب فيك، وهو ما زاد من صعوبة عمل السلطة القضائية كما خلصت أحكام القضاء الأمريكي^(٥).

(١) د. محمد سلامة عبد المنعم، جريمة الانتقام الإباضي عبر تقنية التزييف العميق deepfakes والمسئولية الجنائية عنها، مجلة الحقوق للبحوث القانونية والاقتصادية، جامعة الإسكندرية، عدد ٢(١)، ٢٠٢٢، ص ٣٦٧.

(٢) (<https://spectrum.ieee.org/tech-talk/computing/software/what-are-deepfakes-how-are-they-created>).

(٣) Mathilde Pavis, Rebalancing our regulatory response to Deepfakes with performers' rights, *The International Journal of Research into New Media Technologies*, Vol. ٢٧(٤)، ٢٠٢١، p. ٩٧٦.

(٤) د. مصطفى صلاح عبد الحميد، التزييف الرقمي وأثره على حجية الأدلة الرقمية في الدعاوى الجنائية، دراسة فقهية مقارنة، مجلة الشريعة والقانون، جامعة الأزهر، العدد ٤٠، أكتوبر ٢٠٢٢، ص ٨٥٠.

(٥) Fariss-Borello v. City of Scottsdale, ٢٠١٩ U.S. Dist. LEXIS ١٥٥٠١٣.

ومن التشريعات التي وضعت تعريف للتزييف العميق (الديب فيك)، هو قانون التزييف العميق في ولاية تكساس برقم SB 751 في 18 أبريل 2019، الذي عرف التزييف العميق بأنه " الفعل المرتبط بعمل جريمة جنائية بتصنيع فيديو خادع بهدف التأثير على نتيجة الانتخابات، إلا أن هذا التعريف قد جاء قاصراً، لتركيزه بصورة أساسية على حماية المرشحين للمناصب السياسية^(١).

ومن خلال مطالعة نصوص التشريعات المصرية، لم نقف على تعريف للتزييف العميق (الديب فيك)، غير أنه قد ورد تعريف للتزييف من خلال الفقرة الثانية من نص المادة رقم (202) من قانون العقوبات والتي نصت على أنه: "يعتبر تزييفا انتقاص شيء من معدن العملة أو طلاؤها بطلاء يجعلها شبيهة بعملة أخرى أكثر منها قيمة، ويعتبر حكم العملة الورقية أوراق البنكنوت المأذون بإصدارها قانوناً".

وبذلك نلاحظ على أن المشرع المصري قد ربط مفهوم التزييف بالعملات المعدنية أو الورقية أو أوراق البنكنوت المأذون بإصدارها قانوناً.

وعلى أية حال يمكننا القول بأن تقنية الديب فيك (Deepfake) هي تقنية تستخدم الذكاء الاصطناعي لخلق محتوى مزيف يبدو وكأنه حقيقي، عادةً ما يتم استخدامها لخلق فيديوهات أو صور تظهر أشخاصاً وأحداثاً وأصواتاً وتعابير وجوه تم إنشاؤها بواسطة الكمبيوتر بطريقة تجعلها تبدو وكأنها حقيقية.

وتعتمد تلك التقنية على شبكات عصبية عميقة وتعلم الآلة لمحاكاة السلوك والمظهر البشري، يمكن استخدام الديب فيك لأغراض مختلفة، بما في ذلك السخرية أو الاحتيال أو التلاعب بالمعلومات أو إنتاج محتوى إباحي مزيف.

وعلى الرغم من أن تقنية الديب فيك قد تكون ممتعة من الناحية الإبداعية، إلا أنها أثارت قلقاً كبيراً بسبب استخدامها في الأغراض الضارة والمضرة، مثل نشر معلومات مضللة أو التلاعب بالمعلومات السياسية أو الاعتداء على خصوصية الأفراد.

ولذلك، هناك جهود متزايدة لتطوير تقنيات اكتشاف ومكافحة الديب فيك وتشريعات تنظم استخدامها وتطبيق العقوبات على الاستخدامات غير القانونية.

(١) Lourdes Vazquez, recommendations for regulation of deepfakes in the U.S.: deepfake laws should protect everyone not only public figures <https://spectrum.ieee.org/tech-talk/computing/software/what-are-deepfakes-how-are-they-created>

المطلب الثاني

خصائص تقنية الـديب فيك

تقنية الـديب فيك (Deepfake) هي تقنية متقدمة تعتمد على الذكاء الاصطناعي والتعلم العميق لإنشاء محتوى مزيف يبدو وكأنه حقيقي. تتميز هذه التقنية بعدة خصائص وميزات مهمة، ومن خلال هذا المطلب سوف نقوم بعرض أهم خصائص تقنية الـديب فيك من خلال النقاط التالية:

١ - التعلم العميق (Deep Learning):

تعتبر القدرة على التعلم العميق إحدى مميزات السلوك الذكي، فإنه إن كان التعلم في البشر يتم عن طريق الملاحظة أو الاستفادة من أخطاء الماضي، فإن برامج الذكاء الاصطناعي تعتمد على استراتيجيات "تعليم الآلة"، ويتم التعلم العميق عبر إدخال مجموعة بيانات ضخمة؛ لإيجاد نظريات وخوارزميات، ويكون لديها القدرة على إيجاد أساليب استنباطية عالية عبر تحليل مجموعة البيانات، ومن أمثلة مجالات استعمالاتها: التعرف على الوجه والكلام ومعالجة اللغات الطبيعية والرؤية الحاسوبية^(١).

٢ - المعالجة الكبيرة للبيانات:

لعل التبادل المتزايد للرسائل التي تحتوي على الصور الشخصية أو مقاطع الفيديو أو التسجيلات الشخصية، الذي يقوم بها بعض الأفراد طواعية من خلال مشاركة هذه الرسائل مع الشركاء الحاليين أو المرتقبين، أوجد بيئة ملائمة تضم العديد من البيانات الشخصية الذي يمكن إساءة استخدامها من أجل التهديد أو الاستغلال أو الإيذاء المبهج، ومن صور إساءة الاستخدام تزييف الصور أو الصوت أو الفيديو من خلال تقنية الـديب فيك، ثم مشاركة هذا المنتج المزيف مع الآخرين^(٢).

٣ - توليد الوسائط المتعددة:

تقنية الـديب فيك يمكنها توليد فيديوهات وصور وصوتيات مزيفة، مما يسمح بالتلاعب بمختلف أنواع الوسائط.

ففي يونيو ٢٠١٩ ظهرت فضيحة سياسية تتعلق بفيديو شذوذ جنسي يظهر فيه وزير الشؤون الاقتصادية الماليزي Azmin Ali يمارس اللواط، دافع الوزير وأنصاره ومن بينهم رئيس الوزراء الماليزي بأن الفيديو كان بتقنية الـديب فيك بقصد تخريب حياته السياسية، ومع ذلك لم يتمكن الخبراء الدوليون من العثور على أي

(١) د. أحمد مصطفى معوض محمد محرم، استخدام الذكاء الاصطناعي، استخدام تقنية التزييف العميق في قذف الغير نموذجاً (دراسة فقهية مقارنة معاصرة)، مجلة البحوث الفقهية والقانونية، العدد ٣٩، أكتوبر ٢٠٢٢م - ١٤٤٤هـ، ص ٢٥١٢.

(٢) (Kimberly J. Mitchell. et al, Prevalence and Characteristics of Youth Sexting: A National Study. Pediatrics, vol.١٢٩, no.١, January ٢٠١٢, pp.١٣-٢٠)

مؤشرات على التلاعب بالفيديو^(١).

٤ - تكامل الأصوات والصور:

يمكن دمج صور وأصوات من مصادر مختلفة لإنشاء محتوى دقيق ومقنع، حيث إن التزييف لا يقتصر على فبركة الأحداث من خلال الصور فقط بل يتعداه الأمر إلى تشويه الحقائق وتغيير السياق العام لبعض الأحداث والتلاعب بمقاطع الفيديو مما يسهل تلفيق أقوال وأفعال لشخص ما دون علم منه، بهدف تعزيز بعض الإشاعات والدعاية المغرضة في المجتمع، أو نشر أفكار ومعتقدات لتشكيل رأي ما أو تغيير اتجاهات وأفكار معينة، وقد يتعداه الأمر للسخرية والاستهزاء من بعض الشخصيات سيما السياسية منها، هذا ما قد يؤدي إلى عواقب وخيمة^(٢).

٥ - الواقعية العالية:

حيث تعمل البرامج المستخدمة في الديو فيك عن طريق آلية محددة قادرة على خداع خوارزميات الاكتشاف، وبناء على منافسة بين خوارزميتين: تقوم الأولى بنسخ مقطع فيديو متطابق عدة مرات عن طريق استرداد وجه خارجي إليه، وتكشف الثانية جودة مقاطع الفيديو التي تم انشاؤها بواسطة الخوارزمية الأولى من أجل استبعاد الأقل مصداقية، وهو ما يطلق عليه تقنية "GAN" أي "شبكات الخصومة التوليدية" التي تهدف إلى التدريب على إنشاء محتوى مزيف يشبه المحتوى الأصلي، بحيث تصعب التفرقة بينهما، سواء عن طريق العين البشرية أو الأجهزة الآلية، وبالتالي فإن تقنية الديو فيك تهدف إلى إنشاء مقاطع فيديو واقعية للغاية مع توفير الحماية من الكشف السريع عن المنتج المزيف^(٣).

٦ - التحسين المستمر:

يتم تطوير تقنية الديو فيك بشكل مستمر، مما يزيد من دقتها وواقعيتها، حيث يستخدم الذكاء الاصطناعي الخوارزميات والبيانات التي تمت برمجتها فيه والتي يقوم باستخدامها في اتخاذ القرارات والتنبؤات المستقبلية، ومن هذه الخوارزميات يتعلم الذكاء الاصطناعي حلول للمشكلات والقرارات التي يتعامل معها^(٤).

(١) د. ولاء محمد محروس الناغي، د. ياسر محمد محروس الناغي، إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق "Deep fakes"، المجلة العلمية لبحوث الصحافة، كلية الإعلام، جامعة القاهرة، العدد ٢٤، ٢٠٢٢، ص ٣٩٨.

(٢) حية بلواضح، استخدام تقنية الذكاء الاصطناعي "التزييف العميق" في الفبركة الإعلامية: دراسة تحليلية لعينة من الفيديوهات المنشورة على منصة تويت: الانتخابات الأمريكية لسنة ٢٠٢٠ نموذجاً، رسالة ماجستير، كلية العلوم الإنسانية والاجتماعية، جامعة قاصدي مرباح - ورقلة، الجزائر، ٢٠٢١، ص ٧٣.

(٣) د. أحمد عبد الموجود أبو الحمد زكير، جريمة التزييف الإباحي العميق "دراسة مقارنة"، المجلة القانونية، كلية الحقوق، جامعة القاهرة، فرع الخرطوم، المجلد ١١، العدد ٧، ٢٠٢٢، ص ٢٢٢٧.

(٤) د. خالد ممدوح إبراهيم، التنظيم القانون للذكاء الاصطناعي، دار الفكر الجامعي، الإسكندرية، ٢٠٢٢، ص ٣٧.

٧ - استخدامات متعددة:

يمكن استخدام التقنية لأغراض مختلفة مثل الفنون الإبداعية، والترفيه، والأمان، والأبحاث العلمية، والتلاعب بالمعلومات، والأغراض الضارة.

إلا أن تقنية الديب فيك قد كشفت عن وجهها القبيح والتي تتيح لأي شخص يمتلك مجموعة من الصور والفيديوهات سواء عن طريق البحث في جوجل أو مواقع التواصل الاجتماعي بإدخال البيانات لاستبدال الوجوه وإنتاج مقاطع فيديو مزيفة بشكل لا تشوبه شائبة تقريبا، حيث لا تحتاج التقنية إلى أي إشراف بشري بعد عملية التعلم الآلي الأولية ولكن تواصل الخوارزمية تحسين العمل بشكل مستقل ولا تستطيع العين المجردة كشف التلاعب^(١).

٨ - تحديات أمنية وقانونية:

تواجه تقنية الديب فيك تحديات أمنية وقانونية، فقد أصبح الاحتيال المعلوماتي والأخبار الزائفة مظهرا للثقافة السائدة اليوم؛ حيث يسهل إنتاج هذا المحتوى وتوزيعه؛ مما يرسخ الشك في المجتمع، بل تساءل البعض إن كانت الحقيقة لا تزال موجودة أم أن البشرية تعيش في عصر التزييف والتضليل، لقد ساعدت الحالة السائدة للعالم الرقمي على التوسع في إنتاج الأخبار الكاذبة وانتشارها، وظاهرة الأخبار المجهولة والتحلل من القواعد الأخلاقية والضوابط الاجتماعية للحوار، وولدت الشعور بالإفلات من المحاسبة الذي يشجع على ترويج الشائعة والدعاية بكل أصنافها^(٢).

٩ - مكافحة الديب فيك:

تتم تطوير تقنيات وأدوات لاكتشاف ومكافحة الديب فيك، والتحقق من الأصالة للمحتوى المتداول على الإنترنت.

فعلى سبيل المثال تُستخدم تقنية Eulerian Video Magnification أيضا للتعرف على "الفيديو المزيف" الذي تم إنشاؤه بمساعدة الذكاء الاصطناعي، يعتمد على تفاصيل الصورة العميقة والتعرف على أصغر التفاصيل، مثل وجود أو عدم وجود معدل ضربات القلب لدى البشر، والتغيرات في لون الجلد بسبب تدفق الدم، وما إلى ذلك^(٣).

(١) د. ولاء محمد محروس الناغي، د. ياسر محمد محروس الناغي، مرجع سابق، ص ٣٩٧.

(٢) سعد مفلح حمود، دور أنظمة الذكاء الاصطناعي في مكافحة الشائعات الإلكترونية، المجلة العربية للدراسات الأمنية، جامعة نايف العربية للعلوم الأمنية، المجلد ٣٩، العدد ١، ٢٠٢٣، ص ٨٥، ٨٦.

(٣) د. عمرو إبراهيم محمد الشربيني، تأثيرات تطور تقنيات الذكاء الاصطناعي على العمل الشرطي لمواجهة الحروب النفسية، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، عدد خاص، ٢٠٢١، ص ١٠٢٦.

١٠ - التشريعات والتنظيمات:

هناك تشريعات وقوانين تم وضعها لمحاولة تنظيم استخدام تقنية الـديب فيك وتطبيق العقوبات على الاستخدامات غير القانونية.

فقد سارعت ولاية فرجينيا بفرض عقوبات جنائية على المواد الإباحية المزيفة من خلال التقنيات المعدة لذلك والتي من بينها تقنية التزييف العميق بدون موافقة ذوي الشأن وبقصد الإكراه أو المضايقة أو التخويف، ذلك القانون الذي دخل حيز التنفيذ في ١ يوليو ٢٠١٩، جعل اصطناع أو بيع أو توزيع الصور ومقاطع الفيديو الإباحية المفبركة جنحة من الدرجة الأولى، يُعاقب عليها بالسجن لمدة تصل إلى عام وغرامة قدرها ٢٥٠٠ دولار، وفي الأول من سبتمبر ٢٠١٩، جرمت ولاية "تكساس" هي الأخرى، إنشاء أو توزيع مقاطع فيديو مزيفة من خلال إدخال تعديل على قانون الانتخابات لديها بإضافة نص جديد يُجرم هذا الفعل إذا قُصد منه إيذاء مرشح معين أو التأثير على نتيجة الانتخابات، واعتبرت هذا الفعل كذلك جنحة من الدرجة الأولى يُعاقب مرتكبها بالسجن لمدة عام في أحد سجون الولاية وغرامة تصل إلى ٤٠٠٠ دولار^(١).

(١) د. محمود سلامة عبدالمنعم الشريف، جريمة الانتقام الإباحي عبر تقنية التزييف العميق "Deep fakes" والمسؤولية الجنائية عنها، مجلة كلية الحقوق للبحوث القانونية والاقتصادية، كلية الحقوق، جامعة الإسكندرية، العدد ٢، ٢٠٢٢، ص ٣٧٦، ٣٧٧.

المبحث الثاني

مخاطر تقنية الـديب فيك (Deep fakes) وتطورها

تمهيد وتقسيم:

تكتنف تقنية الـديب فيك مخاطر عديدة من بينها التضليل المعلوماتي، والتلفيق المتعمد، وتشويه الحقائق، والتأثير على السمعة، وقد تبدى ذلك بجلاء في مقاطع الفيديو غير الحقيقية التي اصطنعت للشخصيات العامة، لا سيما الفنانين، كالفديو المفبرك للرئيس الأوكراني "Zelenskyy" الذي انتشر على بعض وسائل التواصل الاجتماعي في مارس ٢٠٢٢، وهو يخبر جنوده بإلقاء أسلحتهم والاستسلام في القتال ضد روسيا، وللمشاهير أيضا كالمقطع المزيف الشهير لـ "Mark Zuckerberg" مؤسس فيسبوك الذي يتفاخر فيه بالسيطرة الكاملة على البيانات المسروقة لمليارات الأشخاص في يونيو ٢٠١٩م^(١).

ومما لا شك فيه أن الأمثلة السابق بيانها ما هي إلا جزء يسير من التهديدات والمخاطر التي يمكن أن تتسبب في إحداثها تقنيات الـديب فيك، وأصبحت مخاطر تقنيات الـديب فيك لا تقتصر على الشخصيات العامة فقط وإنما تمتد أيضًا إلى الأفراد العاديين.

حيث يمكن للأفراد العاديين أن يصبحوا ضحايا لتقنية الـديب فيك عبر إنتاج مقاطع فيديو أو صور مزيفة تهدف إلى تشويه سمعتهم أو تشويه صورتهم، كما يمكن استخدام مقاطع فيديو مزيفة لابتزاز الأفراد العاديين وتهديدهم بنشر المحتوى المزيف إذا لم يتوافقوا على مطالب الابتزاز.

ولا يقف الأمر عند ذلك وإنما تلك التقنيات في تطور مستمر مما يزيد من مخاطر تلك التقنيات، وهو ما سنقوم ببيانه من خلال المطالب الآتية:

المطلب الأول: مخاطر تقنية الـديب فيك (Deep fakes).

المطلب الثاني: تطور تقنية الـديب فيك (Deep fakes).

(١) د. محمود سلامة عبدالمنعم الشريف، مرجع سابق، ص ٣٧٠، ٣٧١.

المطلب الأول

مخاطر تقنية الديوبيك (Deep fakes)

تقنية الديوبيك (Deepfake) هي تقنية تستخدم الذكاء الاصطناعي لإنشاء مقاطع فيديو أو صوتية مزيفة تبدو وكأنها حقيقية بشكل مخادع. يتم ذلك عن طريق دمج ملامح وأصوات أشخاص حقيقيين في مشاهد مفبركة تمامًا. على الرغم من أن هذه التقنية يمكن أن تكون مذهلة من حيث القدرة على إنشاء محتوى إبداعي وترفيهي، إلا أنها تشكل مخاطر كبيرة وتحديات عدة، ومنها:

أولاً: تهديد الأمن المجتمعي:

يمكن استخدام تقنية الديوبيك لإنتاج مقاطع فيديو أو صوتية تظهر شخصًا يقول أو يفعل أشياء لم يفعلها في الواقع. هذا يمكن أن يؤدي إلى نشر أخبار كاذبة ومضللة والتأثير على الرأي العام والسياسة، وهو ما يمثل تهديدًا واضحًا للأمن المجتمعي، وهو ما يمكن بيانه من خلال النقاط التالية:

١ - التهديد السيبراني:

قد يستخدم القراصنة تقنية الديوبيك لإنتاج مقاطع فيديو مزيفة للشركات أو الأفراد ومن ثم يحققون أرباح مالية من خلال الفيديوهات الإباحية.

وقد كانت الممثلات Emma Watson, Gal Gadot, and Taylor Swift من بين أوائل الممثلات التي يتعرض للاستغلال والابتزاز من جانب مستخدمي تقنية الديوبيك، وما زاد من اللجوء إلي تحقيق الأرباح من جانب مستخدمي تقنية الديوبيك هو أن هذه التقنية قد أصبحت متوفرة، ويمكن للمحترفين والمبتدئين على حد سواء^(١)، وقد وجد أن النساء هم الأضعف، ومن السهل تعرضهن للابتزاز نتيجة السلوكيات الاجتماعية المحافظة التي يسهل عليها تصديق تلك الصور أو الفيديوهات التي يتم عملها باستخدام تقنية الديوبيك، وهو ما يسهل تفسير الإحصاءات التي قدرتها مبادرة الحقوق المدنية المعلوماتية التي أجريت عام ٢٠١٤، التي وجدت أن ٩٠٪ من ضحايا الدب فيك من النساء، وأن ٦٨٪ من الضحايا تراوحت فئتهم العمرية ما بين ١٨-٣٠ سنة.

٢ - الانتقام الإباحي:

قد يكون الهدف من استخدام تقنية اديوبيك فيك هو الانتقام من الضحايا أو تهديدهم بالصور الإباحية التي يقوم الجاني باصطناعها لهم. وفي هذا الصدد، تعرف جريمة الانتقام الإباحي بأنها نشر صورة ذات طبيعة إباحية، تم الحصول عليها بصورة مشروعة للمجنى عليه بغرض الانتقام منه بعد انقضاء العلاقة، ويكون نشر هذه

(١) (Keats Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security."

California Law Review ١٠٧, no. ٦, ٢٠١٩, p. ١٧٦٢.

الصورة مصحوباً بتهديد نشر محتوى خاص على وسائل التواصل الاجتماعي إذا لم يتم الاستجابة لمطالب المتهم، وهذه الجريمة من الجرائم المرتبطة بالنوع، التي غالباً ما يكون ضحاياها من النساء^(١).

٣ - الإيذاء المبهج:

الإيذاء المبهج، أو ما يعرف Happy slapping، وفيه يقوم الجاني بتعذيب المجنى عليه بدنياً أو جسدياً وتصويره، ونشر هذه الصور بقصد تحقيق المتعة، الترفيه أو إذلال المجنى عليه، وهناك من الأسباب المختلفة التي تؤدي إلى حدوث هذه الظاهرة، مثل انتشار القدوة السيئة في وسائل الإعلام، التي تظهر من يقوم بمثل هذه الأفعال عزيزاً في نظر أقرانه، التفكك الأسري، تعاطي المخدرات^(٢).

ثانياً: تهديد تقنية الديب فيك للحق في الخصوصية :

تهدد تقنية الديب فيك الحق في الخصوصية، ذلك الحق الذي كفلته القوانين والداستير المختلفة، ذلك التهديد الذي اتخذ مظاهر مختلفة، ووجد له العديد من التطبيقات القضائية، وهو ما يمكننا بيانه على النحو التالي:

١ - مظاهر تهديد تقنية الديب فيك للحق في الخصوصية:

يمكن لتقنيات الديب فيك أن تهدد الحق في الخصوصية، خاصة الخصوصية الجنسية، إذ تصور الأشخاص الذين يتم معالجة صورهم باستخدام الديب فيك في أوضاع منافية للأداب، التي تحدث لهم ازدراء عند أهلهم وذويهم، وهو ما يشكل اعتداء على حق الأفراد في الصورة، وفقاً للضوابط والشروط التي وضعتها المادة ٢٢٦-١ من قانون العقوبات الفرنسي^(٣).

علاوة على هذا التهديد على المستوى الشخصي، فإن تقنية الديب فيك تحدث تهديداً للخصوصية في مجال العمل، إذ تم عمل صورة للسيدة نانسي بيلوسى، رئيسة مجلس النواب في الولايات المتحدة الأمريكية، وهى تتحدث كما لو كانت في حالة سكر، وهو ما أزعج الحكومات، التي اعتبرت أن تقنية الديب فيك تهدد

(١) Putu Adnyana, and Titiek Guntari, Legal protection of women victims of revenge porn based on pornography and ITE Law, *Legal Brief*, Vol. ١١, No ٥, ٢٠٢٢, p. ٣٣٦١.

د. حسام محمد السيد محمد، المواجهة الجنائية لظاهرة الثأر الإباضي، دراسة مقارنة بين النظامين الأنجلو أمريكي واللاتيني، *مجلة الدراسات القانونية والاقتصادية*، عدد ٩ (٥)، ٢٠١٩، ص ٣١.

(٢) د. سمير الجمال، المسؤولية المدنية عن الإيذاء الممنهج، دراسة مقارنة، *مجلة البحوث القانونية والاقتصادية*، العدد ٦٨، ٢٠١٩، ص ٧٧-٢٤٣.

(٣) Isabelle Lories, La protection pénale de la vie privée, Presses Universites d'Aix-Marseille, ١٩٩٩, p.١٠٤.

الديمقراطية^(١)، لذلك فقد أصدرت لجنة الأمن الداخلي في مجلس الشيوخ الأمريكي تقريراً أوضحت فيه أنه يتعين على الحكومة الفيدرالية تحديد الأدوات والتقنيات التي يتم استخدامها في تطوير تقنية الريب فيك، واتخاذ التدابير المضادة لهذه التقنيات، وابتكار الأدوات والأساليب التي يمكن من خلالها كشف المحتوى المزيف الذي تم إنتاجه بواسطة تقنية التزييف العميق، بما يساعد في حماية حق الأفراد في الخصوصية، وهو أمر وجد معه البعض أنه يعكس حجم القلق من توسع تأثير الصور والأفلام التي يتم عملها بواسطة تقنية التزييف العميق على حقوق الأفراد، خاصة الحق في الخصوصية^(٢).

٢ - التطبيقات القضائية لتهديد تقنية الريب فيك للحق في الخصوصية:

هناك العديد من التطبيقات القضائية للتهديد تقنية الريب فيك للخصوصية، من بينها عمل صور إباحية لفتيات قامت بنشر صورهن بحسن نية على الإنترنت، إلا أنهم وذويهم قد فوجئوا بصور إباحية على الإنترنت قام بعض الشبان بعملها باستخدام تقنية الريب فيك، من بينهم فتاة بمحافظة الشرقية، وفتاة أخرى بمحافظة الغربية عام ٢٠٢٢، والتي انتحرت عقب نشر صورتها على مواقع التواصل الاجتماعي، وكان عمل ونشر هذه الصور بغرض الانتقام الإباحي، نتيجة رفض الزواج من هؤلاء الشبان أحياناً، أو لخلافات بين الجيران في أحيان أخرى^(٣).

وأيدت محكمة النقض في مصر حكم محكمة الاستئناف بإدانة المتهم لقيامه بوضع رأس صورة طليقته على صورة جنسية، وكتب تحتها عبارات نابية، وإرسالها عبر البريد الإلكتروني الوهمي الذي أنشأه، اعترف بملكيتها، وأنه لا يعرف غيره كلمة المرور الخاصة به، وفصلت المحكمة في التعويض المؤقت، وإحالة الدعوى المدنية إلى المحكمة المدنية المختصة^(٤)، وأيدت في موضع آخر حكم محكمة الاستئناف بمسئولية الزوج الذي استغل علاقة الزوجية، وقام بتصوير زوجته بملابس تظهر عورتها وقام بنشره عبر الإنترنت، وإرسالها عبر البريد الإلكتروني إلي شهود الإثبات، للتشهير بها^(٥).

وقد وجد لجريمة الانتقام الإباحي العديد من التطبيقات القضائية، إذ قضت محكمة أمريكية في ولاية تكساس بتاريخ ١٥ أغسطس ٢٠٢٣ لصالح أحد الضحايا بتعويض قدره ١,٢ مليار دولار، نتيجة نشر صديق

(١) <https://spectrum.ieee.org/tech-talk/computing/software/what-are-deepfakes-how-are-they-created>

(٢) U.S. Senate, Deepfake Report Act of ٢٠١٩, Rep. No. ١١٦-٩٣, at ٣ (٢٠١٩) , <https://www.congress.gov/١١٦/crpt/srpt٩٣/CRPT-١١٦srpt٩٣.pdf> .

(٣) <https://gate.ahram.org.eg/News/٣٢٣٧٩٥٠.aspx>

(٤) حكم محكمة النقض، الطعن رقم ٤٦٢٩ لسنة ٨٣ ق، جلسة ٢٠١٣/١/٩، مجموعة المبادئ القانونية التي قررتها محكمة النقض في جرائم الاتصالات، المكتب الفني، ٢٠٢١، ص ٦٤.

(٥) حكم محكمة النقض، الطعن رقم ٢٤٦٥ لسنة ٨٣ ق، جلسة ٢٠١٤/١/٦، مجموعة المبادئ القانونية التي قررتها محكمة النقض في جرائم الاتصالات، المكتب الفني، ٢٠٢١، ص ٦٤.

لها صور إباحية التقطها لها، وأرسلها عبر حسابات بريد إلكتروني مزيفة لأصدقائها وزملاءها في العمل، ونشرها على موقع إباحي يمكن للجمهور الوصول إليه، تلك الصور التي سبق وأن حصل عليها أثناء علاقتهما معاً في شيكاغو عام ٢٠١٦^(١)، وفي ١٧ مارس ٢٠١٧ تعرضت عارضة الأزياء الأمريكية ميشا بارتون لانتقام إباحي بعد نشر صور حميمة لها التقطها بكاميرة سرية، وتم عرضها على أحد المواقع الإباحية، وطلبت محامية المجنى عليها التعويض، ومنع نشر مقاطع الفيديو على شبكات التواصل الاجتماعي^(٢).

وفي فرنسا، نجد أن أحكام القضاء قد أرست مبدأ هام، وهو أن الحق في الصورة مستقل عن الحق في حماية الحياة الخاصة، ويمكن أن تقع عليه بعض اعتداءات أثناء الحياة العامة للشخص حتى ولو لم يكن هناك سر يجب المحافظة عليه، ومن ثم فإن التقاط صورة للمجنى عليه في مكان عمله بقصد إجراء المعالجة عليها لا ينفى حق المجنى عليه في الخصوصية^(٣).

(١) <https://www.banany.org>; visited on ١٨ august ٢٠٢٣.

(٢) saidaonline.com, visited on ١٨ august ٢٠٢٣.

(٣) T G.I Graise, ١٤ juin ٢٠٠١.

المطلب الثاني

تطور تقنية الـديب فيك (Deep fakes)

من خلال التتبع التاريخي لنشأة تقنية الـديب فيك أو التزييف المعقد نجد أن هذا المصطلح قد ظهر للمرة الأولى عام ٢٠١٧، في مجال السياسية عندما نشر Buzz Feed بتاريخ ١٧ أبريل ٢٠١٨ فيديو باستخدام طريقة الـديب فيك ليبين للمشاهدين كيف أن هذه الطريقة سهلة ومن الممكن استخدامها من جانب عدد واسع من الناس^(١).

وكانت البدايات الأولى لهذه النشأة مع تصميم Hunter Moores عام ٢٠١٠ موقِعاً على الإنترنت بعنوان IsAnyoneUp، والذي وضع عليه صورة عارية لشريكته وأصدقائه، وتبارى رواد مواقع التواصل الاجتماعي على زيارة هذا الموقع، ووضع صور إباحية عليه، بل هناك من الصور التي كتب تحتها بيانات كاملة من الاسم والعنوان والمهنة وغير ذلك بقصد الانتقام من أصحاب هذه الصور، وقد استمر هذا الموقع ١٦ شهر كان يزوره كل أسبوع قرابة ٣٥ ألف مشاهد، ثم تطورت هذه الفكرة، فلم يعد بالضرورة لأن تكون تلك الصور الإباحية التي يتم نشرها على مواقع التواصل الاجتماعي حقيقية، بل اتجه المتخصصون في علوم الحاسب الآلي إلي تزييف تلك الصور من خلال تقنيات وبرامج خاصة، أهمها تقنية الـديب فيك^(٢).

وتكمن خطورة تقنية الـديب فيك في أنها تمكن الأشخاص من تصوير الغير على أنه فعلوا أفعالاً لم يرتكبوها، ونشرها على وسائل التواصل الاجتماعي، وأن هذه الصور والفيديوهات التي تم عملها تنتشر بسهولة، وذلك بسبب طبيعة وسائل التواصل الاجتماعي، حتى أن هذه الرسائل التي يتم بثها تعرف بالرسائل الفيروسية، تشبهاً لها بالفيروسات التي يمكنها الانتشار بصورة كبيرة إلي عدد واسع من رواد مواقع التواصل الاجتماعي، فضلاً عن الصور التي يتم بثها هذه تكون على درجة من الإلتقان بما يصعب على كثير من الناس، خاصة غير المحترفين منهم تمييزها بأنها مزيفة، فضلاً عن كون هذه الفيديوهات من الصعب حذفها من على مواقع التواصل الاجتماعي.

وفي حقيقة الأمر، فإن نشأة الـديب فيك لم تكن قاصرة على نشر الفيديوهات الإباحية فقط، بل توغل استخدام هذه التقنية في كافة مجالات الحياة، في السياسية، الاقتصاد والفن وغيرها من مجالات الحياة، على سبيل المثال، وفي ٢٠ مايو ٢٠٢٠، تحدثت نانسي بيلوسي، المتحدثة باسم البيت الأبيض في الولايات المتحدة عن فيديو، اتهمت فيه أنصار الرئيس ترامب بعمله باستخدام تقنية الـديب فيك، يصور هذا الفيديو بيلوسي وهي تتحدث كما لو كانت تتحدث وهي في حالة سكر، وذلك في إطار حالة السجال والصراع السياسي العميق بين

(١) (<https://www.youtube.com/watch?v=cQ٥٤GDm١eL٠>)

(٢) Claire Langlais-Fontaine, Démêler le vrai du faux: étude de la capacité du droit actuel à lutter contre les deepfakes, La Revue des droits de l'homme, N°١٨ | ٢٠٢٠, p.١.

نانسى بيلوسى وإدارة الرئيس ترامب، خاصة وأن توقيت عمل هذا الفيديو كان على أعتاب الانتخابات الرئاسية التي جرت عام ٢٠٢٠، التي فاز بها الرئيس جو بايدن الحالي، فكان يحاول كل طرف تصوير الطرف الآخر على أنه غير مسؤول عن تصرفاته، حتى وإن كان ذلك بصورة غير حقيقية، ووجدوا في تقنية الديب فيك وسيلة لتحقيق ذلك^(١).

(١) <https://www.washingtonpost.com/technology/2020/08/03/nancy-pelosi-fake-video-facebook/>

المبحث الثالث

المواجهة التشريعية لمخاطر تقنية الـديب فيك (Deepfakes)

تمهيد وتقسيم:

لا مرأ بأن استخدام تقنية الـديب فيك في الاعتداء على حق الأفراد في الخصوصية والكرامة الإنسانية يستلزم التدخل والمواجهة التشريعية لهذا الاعتداء، وتحتاج المواجهة التشريعية لمخاطر تقنية الـديب فيك إلى جهود متعددة الأوجه تشمل التشريعات الجديدة وتطوير القوانين القائمة لتكون قادرة على التعامل مع هذه التهديدات السيبرانية المتقدمة.

وبذلك يجب أن تكون هناك آليات قانونية تمكن الأفراد والمؤسسات المتضررة من مقاضاة منتجي محتوى الـديب فيك المزيف والمتسببين في أضرار، إلا أن الاختلاف بشأن كيفية وآلية هذا الاعتداء، إذ يري الفقه بوجود عدة مسارات يمكن من خلالها المواجهة التشريعية لاستخدام تقنية الـديب فيك وهو ما يمكننا بيانه على النحو التالي:

المطلب الأول: المواجهة التشريعية لتقنية الـديب فيك من خلال سن تشريع مستقل.

المطلب الثاني: المواجهة التشريعية لتقنية الـديب فيك من خلال تعديل التشريعات الحالية.

المطلب الثالث: أركان جريمة استخدام تقنية الـديب فيك وتحديد أطراف المسؤولية.

المطلب الأول

المواجهة التشريعية لتقنية الـديب فيك من خلال سن تشريع مستقل

نتيجة ما تفرضه تقنيات الـديب فيك من تهديدات ومخاطر على الحياة الخاصة والعامة، انقسمت التشريعات في هذا الخصوص، فهناك من التشريعات التي عالجت تقنية التزييف العميق في قوانين مستقلة، في حين عالجت تشريعات أخرى هذه الظاهرة الإجرامية في قانون العقوبات، وقد تبنى تجريم التزييف العميق في قانون مستقل بإصدار قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨، والذي ميز فيه بين تجريم فعلين:

أولاً: تجريم إحراز برامج أو أدوات أو معدات أو أكواد مرور أو شفرات، وذلك بقصد استخدامها في ارتكاب جريمة من الجرائم المنصوص عليها في هذا القانون، وعاقب على ذلك بالحبس مدة لا تقل عن عامين، وغرامة لا تقل عن ثلاثمائة ألف جنية ولا تزيد عن خمسمائة ألف جنية، أو أيًا من هاتين العقوبتين^(١).

ثانياً: تجريم معالجة المعطيات الشخصية للغير وربطها بمحتوى مناف للآداب أو لإظهارها بطريقة ما من شأنها المساس باعتباره وشرفه، وعاقب على ذلك بالحبس مدة لا تقل عن عامين ولا تزيد عن خمس سنوات، وغرامة لا تقل عن مائة ألف جنية، ولا تجاوز ثلاثمائة ألف جنية، أو إحدى هاتين العقوبتين^(٢).

وكان المشرع المصري قد عالج في المادة ٢/١٧٨ صناعة وترويج الرسوم أو الصور المنافية للآداب، وعاقب عليها بالحبس مدة لا تزيد عن عامين، وغرامة لا تقل عن خمسة آلاف جنية ولا تزيد عن عشرة آلاف جنية أو بإحدى هاتين العقوبتين.

ومن الملاحظ هنا التناقض الواضح في عقوبة الحبس والغرامة في قانون العقوبات وفي قانون مكافحة جرائم تقنية المعلومات، بل أن هذا التناقض في الحد الأدنى للعقوبات المقررة، إلا أن هذا التناقض يمكن إزالته من خلال إعمال قاعدة مفادها أن الخاص يقيد العام.

وسلك المشرع الأمريكي ذات الطريق الذي سلكه المشرع المصري في التجريم في قانون مستقل لتقنية التزييف العميق، فسن قانون جرم للمرة الأولى استخدام تقنيات الـديب فيك كجريمة مستقلة بذاتها إذا ما كان الهدف من استغلالها هو عمل أفلام إباحية بقصد الإكراه والمضايقة والتخويف لأصحابها، وجعلها من جرائم الدرجة الأولى، وقرر لها عقوبة الحبس مدة لا تزيد عن عام، وغرامة لا تقل عن ٢٥٠٠ دولار.

فعلى صعيد الولايات في الولايات المتحدة الأمريكية، فقد عملت على مواجهة تقنية التزييف العميق من خلال تشريعات مستقلة، وحسبنا من ذلك الإشارة إلي توقيع حاكم ولاية كاليفورنيا بتاريخ ٣ أكتوبر ٢٠١٩

(١) المادة ٢٢ من القانون ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات.

(٢) المادة ٢٦ من القانون ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات.

القانون ٦٠٢ AB، المعروف بقانون تصوير الأفراد باستخدام التقنية الرقمية: الاستغلال الجنسي المادي، ويعاقب هذا القانون على استخدام الأفراد تقنية التزييف العميق (الديب فيك) في عمل صور جنسية أو إباحية، أو نشر هذه الصور بدون موافقة المجنى عليهم، إلا أن أسهم النقد قد وجهت إلي هذا القانون لأنه يركز بصورة أساسية على استخدام تقنية الديب فيك في الأغراض الجنسية، وأن تركيز تجريم القانون استخدام الديب فيك في الأغراض الجنسية يحد من الفعالية التشريعية للقانون، لكون تقنية الديب فيك يمكن استخدامها في مجالات أخرى مثل الأحاديث السياسية والتحريض على كراهية الغير^(١).

أما التشريع الآخر الذي عملت ولاية كاليفورنيا من خلاله على انتهاك خصوصية الأفراد من خلال تقنية الديب فيك فهو قانون الانتخابات الذي تم إصداره بتاريخ ٣ أكتوبر ٢٠١٩، الذي عرف بقانون ٧٣٠ AB، الذي عمل على حماية المرشحين من الاعتداء عليهم وعلى حقهم في الخصوصية من خلال استخدام تقنية التزييف العميق.

ومن نقاط القوة في القانون ٧٣٠ AB أنه قدم تعريف أوسع لتقنية التزييف العميق لتشمل المعالجة الصوتية والمرئية، ويعد هذا القانون مظلة حماية أوسع من قانون الانتخابات النافذ في كاليفورنيا، إلا أن ما يؤخذ على هذا القانون انه قصر نطاق تطبيقه على المرشحين لمناصب معينة، ولا يسرى على كل الأفراد، وهو ما يمكن معه دعوة المشرع الأمريكي إلى إدراج التعريف الشامل لتقنية الديب فيك الواردة في القانون ٧٣٠ AB في كل التشريعات الأخرى التي عالجت تقنية الديب فيك، نتيجة تضيق نطاق تطبيق القانون ٧٣٠ AB على المرشحين للمناصب السياسية فقط دون غيرهم من الأفراد.

علاوة على التشريعين سالف الذكر، فقد أدخل عضو الكونجرس Grayson عن ولاية كاليفورنيا، مشروع القانون الذي حمل رقم ١٢٨٠ AB، بتاريخ ٢١ فبراير ٢٠١٩، الذي هدف إلى حماية القاصرين من مخاطر تقنية التزييف العميق، بعد أن قام مقدم مشروع القانون بالإحالة إلي دراسة وجد فيها أن الكثير من القاصرين هم من يرسلون بصور جنسية لهم إلي المواقع الإباحية التي تقوم بمعالجتها باستخدام الديب فيك، وعلى الرغم أن مشروع القانون يتضمن تعريفاً أوسع وأشمل لتقنية التزييف العميق، إلا أنه مشروع القانون لم يوافق عليه الكونجرس. وقد كان هذا القانون يتضمن عقوبة الحبس مدة عام عن إنتاج ونشر الصور باستخدام تقنية الديب فيك^(٢).

(١) AB-٦٠٢ Depiction of individual using digital or electronic technology: sexually explicit material: cause of action, CAL. LEGIS. INFO. (٢٠١٩-٢٠٢٠), https://leginfo.legislature.ca.gov/faces/billStatusClient.xhtml?bill_id=٢٠١٩٢٠٢٠٠AB٦٠٢.

(٢) <https://www.forbes.com/sites/brucelee/٢٠١٨/٠٩/٠٨/here-is-how-much-sexting-among-teens-has-increased/?sh=١c٥٤٤afd٣٦f١>.

وفي تكساس، فقد تم سن قانون التزييف العميق SB ٧٥١ في ١٨ أبريل ٢٠١٩، الذي عرف التزييف العميق بأنه " الفعل المرتبط بعمل جريمة جنائية بتصنيع فيديو خادع بهدف التأثير على نتيجة الانتخابات، إلا أن هذا القانون، كما هو الحال مع القانون AB ٧٣٠ في ولاية كاليفورنيا، الهدف منه حماية المرشحين لمناصب سياسية، كما ركز القانون SB ٧٥١ على التزييف المرئي دون التزييف المسموع^(١).

وفي عام ٢٠١٩، فقد سنت ولاية فرجينيا قانون عرف بقانون النشر غير القانوني أو البيع غير القانوني لصور الغير^(٢)، والذي جرم عمل صور لأحد الأفراد باستخدام تقنية الديو فيك، وذلك إذا ما كان الفرد في حالة عرى، أو عمل صور تكشف عن أجزاء خاصة من جسده، من ثم يكون القانون الذي سنته ولاية جورجيا يتعلق بصنع ونشر الصور في سياق الانتقام الإباحي^(٣).

وفي تقديرنا أن المشرع المصري قد أحسن صنعاً حينما عالج جريمة التزييف العميق (الديو فيك) في قانون مستقل، وإن لم يكن بالاستقلالية الموجودة في القوانين الأمريكية، بما يسبغ مزيداً من الحماية على ضحايا جرائم تقنية التزييف العميق.

(١) <https://capitol.texas.gov/tlodocs/٨٦R/billtext/html/SB٠٠٧٥١S.htm>.

(٢) Virginia Code Annotated § ١٨.٢-٣٨٦.٢.

(٣) <https://law.lis.virginia.gov/vacode/title١٨.٢/chapter٨/section١٨.٢-٣٨٦.٢/>

المطلب الثاني

المواجهة التشريعية لتقنية الـ Deep Fakes من خلال تعديل التشريعات الحالية

الاتجاه الآخر من التشريعات عمل على تعديل التشريعات الموجودة بالفعل، سواء كان قانون العقوبات أو القانون الخاص، كما هو الحال مع المشرع الفرنسي، الذي عالج هذه الظاهرة الإجرامية في المادة ٢٢٦ من قانون العقوبات، وكانت التشريعات الموجودة تميل إلى الحماية المدنية للضحايا أكثر من الحماية الجنائية، إذ رسمت المادة ٢/٩ من قانون ١٧ يوليو ١٩٧٠ طرق إزالة الاعتداء الواقع على خصوصيات الفرد، فأجازت له اللجوء إلى القضاء لاتخاذ التدابير التي من شأنها أن تمنع أو توقف الاعتداء على خصوصية الفرد^(١)، وهو الطريق الذي رسمته المادة ٩ من القانون رقم ١٧ لسنة ١٩٧٠، وتأسيساً على ذلك، قضت محكمة النقض الفرنسية أنه لا يجوز لقاضي المحكمة الكلية استصدار هذه الأوامر التحفظية أو الوقائية ما لم تكن تلك الأفعال المطلوب وقفها تشكل اعتداء على الحق في الخصوصية^(٢).

وقبل هذا التعديل التشريعي في فرنسا، فإن جريمة الانتقام الإباحي لم تكن تخضع لقانون العقوبات، وحسبنا من ذلك الإشارة إلى حكم محكمة استئناف نيمز Nimes الفرنسية التي قضت بالمسؤولية الجنائية للجاني عن الانتقام الإباحي المضروب بنشر صورته على الإنترنت بدون إذن، إلا أن محكمة النقض الفرنسية ببراءة المتهم، ورفض الدعوى المدنية بسبب موافقة المجنى عليه على نشر الصورة الخاصة ذات الطبيعة الجنسية، وأنها غير مجرمة بمقتضى قانون العقوبات، وإنما تخضع للمسائلة بمقتضى المادة ٦ من قانون الثقة في الاقتصاد الرقمي^(٣).

وهو الأمر الذي لاقى مزيد من الانتقاد من جانب الفقه، لكونه ينال من أعراض وسمعة الأفراد، وهو ما يقتضى توفير الحماية لهم، كما أن هذه الصور والفيديوهات من الصعب إزالتها في العصر الرقمي، كما أن الآخرين يمكنهم الاستمرار في نشرها عبر وسائل التواصل الاجتماعي، كما أن جريمة الانتقام الإباحي من الجرائم العمدية التي يستلزم لانعقادها توفر القصد الجنائي العام، وبموجبه تم إضافة المادة ٢٢٦ إلى قانون العقوبات، التي بموجبها تتوفر حالين من الرضا، هما: الرضا على تسجيل الصورة أو محتوى الفيديو، والرضا على نشر، وأن تخلف حالة الرضا الأخيرة ما يجعل نشر هذه الصور بقصد الانتقام الإباحي هو مناط التجريم، الذي تتعدّد معه المسؤولية الجنائية والمسؤولية المدنية التي تدور معا وجوداً وعدم^(٤).

(١) Basile Ader, la protection de la vie privée en droit positif Français, *LEGICOM* ٤(٢٠), ١٩٩٩, p.٧.

(٢) Cass. Civ. ١^{ère} ch., ٤ Oct. ١٩٨٩.

(٣) Cass. Crim. ١٦ mars ٢٠١٦, no.١٥-٨٢.٦٧٦, Bull. Crim. no. ٨٦.

(٤) د. محمد سلامة عبد المنعم، جريمة الانتقام الإباحي عبر تقنية التزييف العميق deepfakes والمسؤولية الجنائية عنها، مجلة الحقوق للبحوث القانونية والاقتصادية، جامعة الإسكندرية، عدد ٢(١)، ٢٠٢٢، ص ٣٩٨.

وفي إطار إسباغ الحماية على حق الأفراد في السمعة والكرامة، عمل المشرع الفرنسي على حماية كرامة المجنى عليه من خلال حظر إعادة نشر أخبار قد تضر بسمعته وشرفه، كما هو الحال مع نشر أخبار عن تعرض المجنى عليه لاعتداء جنسي من أحد أقاربه مثل أبيه أو أخيه، أو من أبيها أو أخيها، وهو الفعل المجرم في المادة ٣٥ مكرر/٤ من قانون الصحافة، وهي المادة المنشأة بالقانون رقم ٥١٦، الصادر في ١٥ يونيو ٢٠٠٠^(١)، والتي تنص على أنه "يعاقب بغرامة قدرها ١٥٠٠٠ يورو كل من نشر بأي طريقة كانت أو أعاد نشر ظروف جنائية أو جنحة، والتي من شأن إعادة نشرها أن يسبب ضرراً جسيماً بكرامة المجنى عليه، ويكون النشر قد تم بدون موافقة المجنى عليه"، لأن نشر هذه الأخبار يسهم في إصابة المجنى عليه بأمراض نفسية، والتي قد تدفع القاصر إلى الانحراف أو التمادي في الانحراف، وتجعل منه مشروع مجرم في المستقبل، بما يسهم في زعزعة استقرار المجتمع، والاعتداء على حقوق المجتمع في منع الجريمة^(٢).

(١) Art. ٣٥ quater. Créé par Loi ٢٠٠٠-٥١٦ du ١٥ Juin ٢٠٠٠, art. ٩٧, JORF ١٦ juin ٢٠٠٠ ; Ordonnance ٢٠٠٠-٩١٦ du ١٩ Septembre ٢٠٠٠, art. ٣, JORF ٢٢ septembre ٢٠٠٠).

(٢) Nérac-Croisier, D.R., Le mineur et la droit pénal, Paris, ١٩٩٧, pp.٢٤٠-٢٤٣.

المطلب الثالث

أركان جريمة استخدام تقنية الـديب فيك وتحديد أطراف المسؤولية

جريمة استخدام تقنية الـديب فيك (Deepfake) تمثل تحديًا جديدًا ومعقدًا في عصر التكنولوجيا الحديثة، حيث تعتمد على تلاعب بالصوت والصورة بواسطة الذكاء الاصطناعي لإنشاء مقاطع فيديو أو ملفات صوتية تبدو وكأنها تمثل أشخاصًا حقيقيين، ولفهم حقيقة الجريمة وتحديد أطراف المسؤولية، يمكن تناول هذا المطلب من خلال النقاط التالية:

أولاً: أركان جريمة استخدام تقنية الـديب فيك:

١ - الركن المادي (الفعل المحرم)

يعد الركن المادي أحد الدعائم التي تقوم عليها المسؤولية الجنائية، والركن المادي هو المظهر الخارجي الذي تقوم به الجريمة إلى حيز الوجود، وهو الفعل المحرم بموجب نصوص قانون العقوبات أو أحد القوانين الخاصة، إذ يعد الركن الماضي هو تجسيد للإرادة الإجرامية لفاعله^(١).

وغني عن البيان أن الركن المادي له ثلاثة عناصر، وهم السلوك والنتيجة وبينهما رابطة السببية، غير أن عنصر السلوك في التزييف العميق يمر بمراحل متعددة^(٢)، كل مرحلة فيه جريمة مستقلة بذاتها، تبدأ تلك المراحل بسحب وتجميع البيانات الشخصية للضحية من صور وتسجيلات صوتية وفيديوهات سابقة أيا كان مصدرها^(٣)، أما المرحلة الثانية فهي اصطناع مقطع الفيديو من خلال معالجة البيانات التي تم جمعها سلفاً بواسطة معادلات وخوارزميات الذكاء الاصطناعي لإنتاج مقطع فيديو مزيف للمجني عليه، وأخيراً إظهار هذا الفيديو^(٤).

وقد نصت المادة ٢٦ من القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات على أنه "يعاقب... كل من تعمد استعمال برنامج معلوماتي أو تقنية معلومات في معالجة معطيات شخصية للغير لربطها بمحتوى مناف للآداب العامة، أو لإظهارها بطريقة من شأنها المساس باعتباره وشرفه.

(١) د. ضاري خليل، الوجيز في شرح قانون العقوبات، دار القادسية للنشر والطباعة والتوزيع، بغداد، ٢٠٠٥، ص ٦٦.

(٢) الجريمة متتابعة الأفعال تتكون من عدة أفعال مستقلة، يصلح كل منها لإقامة جريمة مستقلة، غير أنه يشترط التقارب بين تلك الأفعال لاعتبارها جريمة واحدة. نقض جنائي ٩ نوفمبر ١٩٩٤، مجموعة أحكام النقض، س ٤٥، ق ١٥٢، ص ٩٨٣.

(٣) وطبقاً للمادة ٢ من القانون رقم ١٥١ لسنة ٢٠٢٠ فإن جمع البيانات الشخصية أو معالجتها أو الإفصاح عنها أو إفشائها بأي وسيلة من الوسائل محظور إلا بموافقة صريحة من الشخص المعني بالبيانات أو في الأحوال المصرح بها قانوناً.

(٤) للمزيد راجع د. محمود سلامة عبدالمنعم، جريمة الانتقام الإباحي عبر تقنية التزييف العميق "Deepfakes" والمسؤولية الجنائية عنها، مجلة كلية الحقوق، جامعة الإسكندرية، المقالة ٥، المجلد ٢٠٢٢، العدد ١، يوليو ٢٠٢٢، ص ٤٠٥ وما بعدها.

٢ - الركن المعنوي (القصد الجنائي)

من المتفق عليه فقهاً وقضاء بأن كل جريمة يستلزم لقيامها وجود ركناً معنوياً، والذي يترتب عليه المسؤولية الجنائية عن هذه الجريمة^(١)، وجريمة التزييف العميق من الجرائم العمدية، وذلك استناداً إلى نص المادة ٢٦ ، والتي نصت على أن "يعاقب ... كل من تعمد استعمال برنامج معلوماتي..."، وبذلك يجب أن يكون الجاني عالماً بالتزييف الحادث وأن تتجه إرادته لإحداث هذا النشاط أو السلوك.

ونلاحظ أن المشرع المصري لم يتطلب قصداً خاصاً، وإنما اكتفى بتوافر القصد العام، وبالتالي يستوى أن يتم هذا التزييف بهدف الانتقام أو الارتزاق أو لأي غرض آخر ، وبذلك لا عبء بين القصد الجنائي وبين الباعث على ارتكاب الجريمة^(٢).

وبذلك يلزم لقيام القصد الجنائي علم الجاني بكافة الوقائع المادية التي تدخل في البنيان القانوني للجريمة^(٣)، وهو ما يتطلب ذلك الرجوع إلى النموذج القانوني للجريمة واستخلاص ما يعد داخلياً في بنائها من وقائع^(٤). والأصل العام هو انصراف العلم إلى كل واقعة يقوم عليها كيان الجريمة، ذلك أن القصد الجنائي يعنى اتجاه الإرادة الواعية إلى الجريمة في كل أركانها وعناصرها، فإذا تطلب القانون العلم بواقعة لتوفر القصد الجنائي، فمعنى ذلك أن الجهل أو الغلط المتعلق بها منافي لهذا القصد، وبالتالي لا يسأل الجاني عن فعله، فالجهل بهذا النوع من الوقائع أو الغلط فيها يعد جهلاً أو خطأً جوهرياً ينتفى به القصد الجنائي^(٥).

ثانياً: أطراف المسؤولية لجريمة استخدام تقنية الـديب فيك:

لما كانت جريمة استخدام تقنية الـديب فيك تتم طبقاً لمراحل متعددة كلا منها يصلح كجريمة مستقلة بذاتها، فإننا يمكننا القول بأن أطراف المسؤولية هم:

١ - متصيد البيانات الشخصية:

فطبقاً للمادة ٢ من قانون البيانات الشخصية سالف البيان، فإن هذا السلوك مجرم، ويعد الفاعل هنا مساهماً تبعياً بالمساعدة؛ إذ أنه قدم البيانات الشخصية لمنتج الفيديو المزيف.

(١) Hosni, M.N., L' Erreur de droit et son influence sur la responsabilité pénale, *Rev. Sc. Crim.*, Vol., ٤, ١٩٩٩, p.٧١١.

(٢) د. أحمد عوض بلال، مبادئ قانون العقوبات المصري، القسم العام، دار النهضة العربية، ٢٠٠٩، ص ٦٦٨.

(٣) د. أشرف توفيق شمس الدين، المسؤولية الجنائية و الركن المعنوي للجريمة، الضوابط الدستورية لنصوص التجريم والعقاب في قضاء المحكمة الدستورية العليا، *مجلة الدستورية*، العدد ١٤، ٢٠٠٨، ص ١٧.

(٤) د. أحمد عوض بلال، مبادئ قانون العقوبات المصري، القسم العام، دار النهضة العربية، ٢٠٠٩، ص ٦٧٠.

(٥) د/ أحمد شوقي أبو خطوة: شرح الأحكام العامة لقانون العقوبات لدولة الإمارات العربية المتحدة، دار النهضة العربية، ص ٢٠٩.

٢ - إنتاج الفيديو المزيف:

وطبقا للمادة ٢٦ من القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات فإن مستخدم البرنامج معلوماتي مسئول جنائيا متى تعمد معالجة المعطيات الشخصية للغير وربطها بمحتوى مناف للأداب العامة، أو لإظهارها بطريقة من شأنها المساس باعتباره وشرفه.

٣ - اظهار الفيديو المزيف:

وطبقا للمادة ٢٥ من القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات فإن الاعتداء على القيم والمبادئ الأسرية في المجتمع المصري، وكذلك انتهاك خصوصية الأفراد ونشرها متى كانت صحيحة أو غير صحيحة يعد جريمة.

الخاتمة

بهذه الكلمات انتهيت بفضل الله وتوفيقه من إعداد هذا العمل البحثي، والذي تم بعنوان "المواجهة الجنائية لتقنية الديو بيك (Deep fakes)"، من خلال ثلاثة مباحث تمت على النحو السابق بيانه، وقد توصلنا من خلال هذه الدراسة إلى عدد من النتائج والتوصيات نوجزها فيما يلي:

النتائج:

- تمكنت تقنية الديو بيك من إنشاء محتوى مزيف يبدو وكأنه حقيقي بشكل مذهل، مما يزيد من خطر تلاعب المعلومات وانتشار الأخبار المزيفة.
- قد تُستخدم التقنية لتزييف تصريحات وتصرفات الشخصيات السياسية والعامّة، مما يمكن أن يؤدي إلى تأثير كبير على القرارات السياسية وتشكيل الرأي العام.
- يمكن استخدام تقنية الديو بيك لإنشاء مقاطع فيديو مزيفة تظهر أشخاصًا في مواقف خاصة أو مخلة بالخصوصية، مما يشكل تهديدًا للخصوصية الفردية.
- تزايدت مخاوف من أن يتم استخدام تقنية الديو بيك في هجمات سيبرانية واختراقات أمنية للتضليل والتلاعب بالمعلومات.
- قد يتم استخدام تقنية الديو بيك لإنتاج أدلة مزيفة في القضايا القانونية أو الجنائية، مما يضعف نظام العدالة ويجعل من الصعب التحقيق في الجرائم.
- زادت الحاجة إلى تعزيز الوعي بمخاطر تقنية الديو بيك وتطوير أدوات للتحقق من صحة المحتوى المتداول على الإنترنت.

التوصيات

- يجب على المشرع العمل على توسيع نطاق الأفعال التي تشكل أفعال التزييف العميق (الديو بيك) بما يمنع الإفلات من العقاب.
- ينبغي زيادة الاستثمار في الأمن السيبراني لحماية البيانات والأنظمة الحيوية من هجمات تستخدم deepfakes.
- يجب تعزيز التعاون الدولي لمواجهة تقنية الديو بيك، حيث يمكن للدول والمنظمات الدولية تبادل المعلومات والخبرات وتطوير استراتيجيات مشتركة.
- يجب تطوير أدوات تحقق أوتوماتيكية وذكية للكشف عن deepfakes، ويمكن أن تستخدم التقنيات الذكية والذكاء الاصطناعي لتحليل الصوت والصورة واكتشاف أي تغييرات غير طبيعية.

قائمة المراجع

أولاً: المراجع باللغة العربية:

- حية بلواضح، استخدام تقنية الذكاء الاصطناعي "التزييف العميق" في الفبركة الإعلامية: دراسة تحليلية لعينة من الفيديوهات المنشورة على منصة تويتر: الانتخابات الأمريكية لسنة ٢٠٢٠ نموذجاً، رسالة ماجستير، كلية العلوم الإنسانية والاجتماعية، جامعة قاصدي مرباح - ورقلة، الجزائر، ٢٠٢١.
- د. أحمد عبد الموجود أبو الحمد زكير، جريمة التزييف الإباحي العميق "دراسة مقارنة"، المجلة القانونية، كلية الحقوق، جامعة القاهرة، فرع الخرطوم، المجلد ١١، العدد ٧، ٢٠٢٢.
- د. أحمد مصطفى معوض محمد محرم، استخدام الذكاء الاصطناعي، استخدام تقنية التزييف العميق في قذف الغير نموذجاً (دراسة فقهية مقارنة معاصرة)، مجلة البحوث الفقهية والقانونية، العدد ٣٩، أكتوبر ٢٠٢٢ - ١٤٤٤هـ.
- د. حسام محمد السيد محمد، المواجهة الجنائية لظاهرة الثأر الإباحي، دراسة مقارنة بين النظامين الأنجلو أمريكي واللاتيني، مجلة الدراسات القانونية والاقتصادية، عدد ٩ (٥)، ٢٠١٩.
- د. خالد ممدوح إبراهيم، التنظيم القانون للذكاء الاصطناعي، دار الفكر الجامعي، الإسكندرية، ٢٠٢٢.
- د. سمير الجمال: المسؤولية المدنية عن الإيذاء الممنهج، دراسة مقارنة، مجلة البحوث القانونية والاقتصادية، العدد ٦٨، ٢٠١٩.
- د. عمرو إبراهيم محمد الشربيني، تأثيرات تطور تقنيات الذكاء الاصطناعي على العمل الشرطي لمواجهة الحروب النفسية، مجلة البحوث القانونية والاقتصادية، كلية الحقوق، جامعة المنصورة، عدد خاص، ٢٠٢١.
- د. محمد سلامة عبد المنعم، جريمة الانتقام الإباحي عبر تقنية التزييف العميق deepfakes والمسؤولية الجنائية عنها، مجلة الحقوق للبحوث القانونية والاقتصادية، جامعة الإسكندرية، عدد ٢ (١)، ٢٠٢٢.
- د. محمد سلامة عبد المنعم، جريمة الانتقام الإباحي عبر تقنية التزييف العميق deepfakes والمسؤولية الجنائية عنها، مجلة الحقوق للبحوث القانونية والاقتصادية، جامعة الإسكندرية، عدد ٢ (١)، ٢٠٢٢.
- د. محمد شوقي العناني، د. إسلام هديب، الذكاء الاصطناعي ودوره في مكافحة الفساد، دار النهضة العربية، القاهرة، ٢٠٢٢م.
- د. محمود سلامة عبدالمنعم الشريف، جريمة الانتقام الإباحي عبر تقنية التزييف العميق "Deep fakes" والمسؤولية الجنائية عنها، مجلة كلية الحقوق للبحوث القانونية والاقتصادية، كلية الحقوق، جامعة الإسكندرية، العدد ٢، ٢٠٢٢.

- د. مصطفى صلاح عبد الحميد، التزييف الرقمي وأثره على حجية الأدلة الرقمية في الدعاوى الجنائية، دراسة فقهية مقارنة، *مجلة الشريعة والقانون*، جامعة الأزهر، العدد ٤٠، أكتوبر ٢٠٢٢.
 - د. ولاء محمد محروس الناغي، د. ياسر محمد محروس الناغي، إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق "Deep fakes"، *المجلة العلمية لبحوث الصحافة، كلية الإعلام، جامعة القاهرة*، العدد ٢٤، ٢٠٢٢.
 - سعد مفلح حمود، دور أنظمة الذكاء الاصطناعي في مكافحة الشائعات الإلكترونية، *المجلة العربية للدراسات الأمنية، جامعة نايف العربية للعلوم الأمنية، المجلد ٣٩، العدد ١، ٢٠٢٣*.
- ثانيا: المراجع باللغة الأجنبية:

- **Basile Ader**, la protection de la vie privée en droit positif Français, *LEGICOM* ٤(٢٠), ١٩٩٩.
- **Claire Langlais-Fontaine**, Démêler le vrai du faux: étude de la capacité du droit actuel à lutter contre les deepfakes, *La Revue des droits de l'homme*, N°١٨, ٢٠٢٠.
- **Elena Igorevna Galyashina, Vladimir Dmitrievich Nikishin**, The protection of megascience projects from deepfake technologies threats: information law aspects, *Journal of Physics: Conference Series*, ٢٠٢٢.
- **Isabelle Lolies**, La protection pénale de la vie privée, *Presses Universites d'Aix-Marseille*, ١٩٩٩.
- **Keats Citron**, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." *California Law Review* ١٠٧, no. ٦, ٢٠١٩.
- **Kimberly J. Mitchell**. et al, Prevalence and Characteristics of Youth Sexting: A National Study. *Pediatrics*, vol.١٢٩, no.١, January ٢٠١٢.
- **Majid Yar, Jacqueline Drew**, Image-Based Abuse, Non-Consensual Pornography, Revenge Porn: A Study of Criminalization and Crime Prevention in Australia and England & Wales, *International Journal of Cyber Criminology*, Vol ١٣ Issue ٢ July – Dec. ٢٠١٩.
- **Mathilde Pavis**, Rebalancing our regulatory response to Deepfakes with performers' rights, *The International Journal of Research into New Media*

Technologies, Vol. ٢٧(٤), ٢٠٢١.

- **Nérac–Croisier**, D.R., *Le mineur et la droit pénal*, Paris, ١٩٩٧.
- *Nicola Henry*, Anastasia Powell & Asher Flynn: Not Just ‘Revenge Pornography’: Australians’ Experiences of Image–Based Abuse, RMIT University, may ٢٠١٧.
- **Putu Adnyana**, and Titiek Guntari, Legal protection of women victims of revenge porn based on pornography and ITE Law, *Legal Brief*, Vol. ١١, No ٥, ٢٠٢٢.
- Rapport: The State Of Deepfakes: Landscape, Threats and Impact, Deeptrace, ٢٧ septembre ٢٠١٩, PP.١–٣
- Robert Chesney, and Danielle Citron, Deepfakes and the new disinformation war: The coming age of post–truth geopolitics. *Foreign Affairs*, ٢٠١٩, ٩٨, ١٤٧.
- Scott R. Stroud: The Dark Side of the Online Self:A Pragmatist Critique of the Growing Plagueof Revenge Porn, *Journal of Mass Media Ethics*, ٢٩(٣), ٢٠١٤.
- **Stephanie Chant**, Majeed Khader, Jansen Ang, Eunice Tan, Katharine Khoo and Jeffery Chin, Understanding, Happy slapping, *Int. J. Police Science and Management*, Vol. ١٤(١), ٢٠١٢.