جريمة الانتقام الإباحي عبر تقنية التزييف العميق "Deepfakes" والمسؤولية الجنائية عنها

دكتور

محمود سلامة عبد المنعم الشريف

دكتوراه في القانون الجنائي – جامعة الإسكندرية

أولاً: المقدمة: مفهوم تقنية التزييف العميق "Deepfakes":

ما من شك أن ثمّة ضرورة لمواكبة القانون الجنائي ما يُستجد من أفعال تُمثل خطراً على المصالح الجوهرية الجديرة بالحماية في مجتمعاتنا، وبخاصة في عصر تتسارع فيه أوجه التكنولوجيا ربما بصفة لحظية، نحو ابتكار العديد من التقنيات الحديثة التي تثير بقدر أهميتها وأحياناً ضروريتها، مخاوف وشكوك كثيرة.

واحدة من هذه التقنيات هي تقنية "التزييف العميق- Deepfakes"، التي يُمكن من خلالها اصطناع مقاطع فيديو مزيفة لأشخاص ما يصعُب وربما يستحيل أحياناً اكتشاف تزييفها كذلك صور وتسجيلات صوتيه[1] تلك

---

[1] في سبتمبر 2019، أنشأ مجرمو الإنترنت صوتاً مزيفاً لرئيس تنفيذي للاتصال بشركته ومطالبتهم بتحويل 243000 دولار إلى حسابهم المصرفي وهو ما أفصح عنه التحقيق الذي نشرته صحيفة The Wall Street Journal تحت عنوان " Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case, Scams using artificial intelligence are a new challenge for companies" بتاريخ 30 أغسطس 2019، على الرابط المرفق بتاريخ دخول 2 أبريل 2020م، الساعة 4:15 عصراً:

https://bit.ly/3sr1RkE

وفي واقعة أخرى حدثت في يناير 2020م تلقي مدير فرع أحد البنوك في الإمارات مكالمة هاتفية مزيفة باستخدام تقنية "التزييف العميق" لأحد أصحاب الشركات المتعاملة مع البنك، وطُلب فيها منه تحويل مبلغ 199،987.75 دولارًا أمريكيًا و215،985.75 دولارًا أمريكيًا على التوالي، وهو ما قام به البنك إلى أن اتضح بعد ذلك ان الواقعة مزيفة بكاملها. على الرابط المرفق بتاريخ دخول 2 إبريل 2020م، الساعة 4:20 عصراً:

Martin Anderson: Deepfaked Voice Enabled $35 Million Bank Heist in 2020, Available at; https://www-unite-ai.translate.goog/deepfaked-voice-enabled-35-million-bank-

الجرائم التي صُنفت ضمن الأخطر في مجال الذكاء الاصطناعي[1]، وتعتمد تلك التقنية الحديثة على "التعلُّم العميـق – Deep Learning"، و"التعلم الآلي– Machine Learning"[2]، كأداتين لفحص تعابير الوجه وحركات الشخص المراد تزييفه مثل الابتسامة ونظرة العين والإيماءة وحركة الشفاه، وتجميع صوراً لوجهه ونبرات الصوت[3]، ثم يتم بعد ذلك تغذية التطبيق بها، على سبيل المثال تطبيق "FakeApp" و"Zao" و"DeepFace Lab" و" Face Swap"، لتنتج لنا مقاطع فيديو مُماثلة للتعبيرات والحركات بشكل

---

heist-in-2020/?_x_tr_sl=en&_x_tr_tl=ar&_x_tr_hl=ar&_x_tr_pto=op,sc

[1] وذلك بحسب دراسة حديثة أعدتها كلية لندن الجامعية في أغسطس 2020 تحت عنوان "'Deepfakes' ranked as most serious AI crime threat " على الرابط التالي بتاريخ دخول 10/ أكتوبر/ 2020، الساعة 5 مساء:

https://www.ucl.ac.uk/news/2020/aug/deepfakes-ranked-most-serious-ai-crime-threat

[2] Nguyen, Thanh & Nguyen, Cuong M. & Nguyen, Tien & Duc, Thanh & Nahavandi, Saeid. Deep Learning for Deepfakes Creation and Detection: A Survey.2019. Available at; https://arxiv.org/pdf/1909.11573.pdf

[3] Lyu, S. Detecting deepfake videos in the blink of an eye. (29, August 2018). Available at; http://theconversation.com/detecting-deepfake-videosin-the-blink-of-an-eye-101072

طبيعي مُسجلة لشخصيات عامة يتكلمون، تبدو واقعية للغاية، مع أنهم في الحقيقة لم ينطقوا بكلمة واحدة مما جاء فيها[1].

من ثم يُمكن القول بأن التزييف العميق عبارة عن نسخة متطرفة مُلفّقة وهمية من بيانات سمعية وبصرية تم التلاعُب بها من خلال أحد تطبيقات الذكاء الاصطناعي المُعدّة لذلك[2]، والذي يعني في جوهره "التقوّل على شخص بشيء لم يقله بواسطة تقنيات تكنولوجية حديثة"[3]. وبحسب البرلمان الأوروبي فالتزييف العميق له مدلول أوسع من الوسائط الحوسبية المركبة التي تقف عند حد تعديل أو تنميط البيانات الأصيلة، إذ يستهدف توليد وتقليد صوت أو صورة أو فيديو بواسطة الذكاء الاصطناعي لا علاقة له بحقيقة الواقع من خلال استنساخ الصوت أو تحريف الصورة أو تركيب النص[4].

---

(1) Chesney, R., and Citron, D. Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. Foreign Affairs, 2019, 98, 147.

(2) Stephen Davies. Deepfakes are the evolution of fake news and are equally as dangerous. Available at; https://www.stedavies.com/deepfakes/

(3) ماري شروتر: الذكاء الاصطناعي ومكافحة التطرف العنيف: كتاب تمهيدي، الشبكة العالمية للتطرف والتكنولوجيا GNET، المركز الدولي لدراسة الراديكالية، كينجز كوليدج لندن، بدون سنة نشر، ص17.

(4) The term deepfake is mostly used to refer to AI-generated video-graphic media. Deepfakes are commonly seen as a specific branch of a broader spectrum of computer-generated content known as

تكتنف تقنية "التزييف العميق- deepfakes" مخاطر عديدة من بينها التضليل المعلوماتي، والتلفيق المتعمد، وتشويه الحقائق، والتأثير على السمعة، وقد تبدى ذلك بجلاء في مقاطع الفيديو غير الحقيقية التي اصطُنعت للشخصيات العامة، لاسيما الفنانين كالفيديوهات المفبركة للممثل الأمريكي "Tom Cruise"[1]، وكذلك السياسيين كواقعة الفيديو المزيف لـ "Nancy Pelosi" رئيسة مجلس النواب الأمريكي وهي ثَمِلة في مايو 2019[2]، والفيديو المفبرك للرئيس الأوكراني "Zelenskyy" الذي انتشر

'synthetic media'. The meaning of the word 'synthetic' in this term is similar to 'synthetic rubber'. It signals that the term encompasses imitations of text, audio-, photo- and video-graphic materials that are perceived as authentic. In popular media, the terms deepfake and synthetic media are seemingly interchangeable, for example, describing AI-generated voice as 'deepfake voice' or 'synthetic voice'. Tackling deepfakes in European policy, Panel for the Future of Science and Technology, European Parliamentary Research Service, Scientific Foresight Unit (STOA), PE 690.039 – July 2021, p.2.

(1) حيث انتشرت مقاطع عديدة للفنان "توم كروز" على من خلال برنامج "TikTok" على الرابط التالي بتاريخ دخول 14-3-2021، الساعة 12:00 ظهراً: https://www.tiktok.com/@deeptomcruise?، كذلك على "YouTube" على الرابط التالي: https://www.youtube.com/watch?v=iyiOVUbsPcM

(2) حيث تم تحرير مقطع فيديو لخطاب "تانسي بيلوسي" في حديثها بمركز التقدم الأميركي في مايو 2019م أثناء الانتخابات الأمريكية، هذا الفيديو المفبرك جعل صوتها بطيء نوعاً وحركاتها غير متزنة مما أعطى صورة للمشاهد بكونها في حالة سُكر، كما لو كانت تحت تأثير الكحول، تم عرض هذا الفيديو على صفحة "Facebook Politics

على بعض وسائل التواصل الاجتماعي في مارس 2022[1]، وهو يخبر جنوده بإلقاء أسلحتهم والاستسلام في القتال ضد روسيا، وللمشاهير أيضاً كالمقطع المزيف الشهير لـ"Mark Zuckerberg" مؤسس فيسبوك الذي يتفاخر فيه بالسيطرة الكاملة على البيانات المسروقة لمليارات الأشخاص في يونيو 2019[2]، هؤلاء الأشخاص تتوفر لهم بيانات صوتية ومرئية وصور وفيديوهات عديدة على شبكة الإنترنت، تلك البيانات الرقمية استُخدمت كوقود لإنشاء فيديوهات مزيفة من خلال تقنية التزييف العميق.

الأمثلة سالفة الذكر ما هي إلا غيضٌ من فيض، إذ إن مخاطر تلك التقنية الحديثة لا تقف عند الشخصيات العامّة فحسب، وإنما أصبحت تمتد

"WatchDog" ثم على يوتيوب والذي رآه 2.5 مليون مشاهد في أقل من أسبوع. يرجع في ذلك إلى الموقع الإخباري "cbsnews" على الرابط التالي:

https://www.cbsnews.com/news/doctored-nancy-pelosi-video-highlights-threat-of-deepfake-tech-2019-05-25/

كذلك أطلقت فيديوهات مفبركة بذات التقنية لكل من الرئيس الأميركي دونالد ترامب والرئيس الروسي فلاديمير بوتين والرئيس السابق باراك أوباما والسيدة الأولى السابقة والمرشحة الرئاسية السابقة هيلاري كلينتون وغيرهم.

[1] Deepfake video of Zelenskyy could be 'tip of the iceberg' in info war, experts warn, Bobby Allyn, , Available at: March 16, 2022, https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia

[2] كما هو منشور على "YouTube" على الرابط التالي؛ بتاريخ دخول 15-3-2021، الساعة 12:00 ظهراً

https://www.youtube.com/watch?v=Ox6L47Da0RY

حتى للأفراد العاديين[1]، ويعزّي تلك المخاطر ثلاثة عوامل رئيسية، **الأول؛** هو عولمة البيانات الشخصية التي أصبحت متوفرة بغزاره على شبكة الإنترنت، على وجه الخصوص، في وسائل التواصل الاجتماعي فغدى من السهل الحصول على صور وفيديوهات وأصوات لشخص ما يُمكن استعمالها في تزييف مقاطع فيديو له. أما **الثاني؛** هو مُرتبط بفكرة الإتاحة، أي إتاحة التطبيقات الخاصة بالتزييف العميق، حتى أصبحت في متناول الجميع دون أن تكون حِكراً على الشركات التقنية الكبرى أو الجهات السيادية أو وسائل الإعلام أو شركات الترفيه وصناعة السينما وغيرها، مما يُعطي الفرصة لأي شخص في استخدامها بمجرد تثبيت تلك التطبيقات على هاتفه اللوحي أو جهاز الكمبيوتر الخاص به[2]. أما **الثالث؛** هو عدم الاحترافية أو ضحالة التخصص، فتلك التطبيقات أصبحت تُخاطب عوام الناس ولا تحتاج

---

[1] ففي أحد الوقائع تم تحويل مبلغ 243 ألف دولار إلى حساب مصرفي في المجر عام 2019م. حيث اعتقد الرئيس التنفيذي لفرع شركة طاقة مقرها المملكة المتحدة، أن الشخص الموجود على الطرف الآخر من الخط هو رئيسه، الرئيس التنفيذي للشركة الأم. وطلب المخادع، الذي استعان بتقنية التزييف العميق، من الرئيس التنفيذي للشركة الفرعية إرسال الأموال إلى مورد مجري على وجه السرعة من خلال أحد تطبيقات التزييف العميق.

Damiani, J. A voice deepfake was used to scam a CEO out of $243,000. Available at https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voicedeepfake-was-used-to-scam-a-ceo-out-of-243000/

[2] Dave Gershgorn, Google Gave the World Powerful AI Tools, and the World Made Porn with Them, QUARTZ. Available at: Google gave the world powerful open source AI tools, and the world made porn with them — Quartz (qz.com)

لمبرمجين أو مطورين برامج لتشغيلها وتوليد فيديو مفبرك أو مصطنع وإنما يتم ذلك من خلال تتابع خطوات بسيطة من خلال التطبيقات الخاصة بها[1].

بيد أن إساءة استعمال تقنية التزييف العميق متعددة كاستعمالها في الأغراض السياسية غير المشروعة لاسيما التأثير على العملية الانتخابية، أو تأجيج العنصرية، أو ازدراء الأديان، أو التشهير بسمعة الأشخاص وانتهاك خصوصياتهم، أو استغلال بياناتهم بموجب تلك التقنية دون رضائهم، ولا أدل على ذلك بما أفصح به تقرير الأمن السيبراني الصادر عن مؤسسة "Startup Deeptrace" الهولندية في عام 2019، بأن إجمالي ما عثرت عليه هو 14678 فيديو مزيف على شبكة الإنترنت في 10 أشهر فقط منذ ديسمبر 2018 وحتى أكتوبر 2019، منها 96% كانت لمواد إباحية شوهدت من قبل 134 ملايين شخصاً[2]. الأمر الذي يُثير الانتباه حول خطورة اصطناع فيديو إباحي مزيف لأشخاص عاديين لمجرد أنهم قاموا بنشر صورهم بحسن نية على أحد وسائل التواصل الاجتماعي ومدى تأثير ذلك على حقهم في الشرف والاعتبار وهو ما حدث بالفعل في عام 2018، حيث اكتشفت طالبة في مدرسة ثانوية أسترالية أن شخصًا ما أدخل وجهها في

---

(1) M. Caldwell, J. T. A. Andrews, T. Tanay, L. D. Griffin. **AI-enabled future crime**. *Crime Science*, 2020; 9 (1) DOI: 10.1186/s40163-020-00123-8. Available at: https://crimesciencejournal.biomedcentral.com/articles/10.1186/s40163-020-00123-8

(2) IVAN MEHTA. A new study says nearly 96% of deepfake videos are porn. Oct 7, 2019. Available at: https://thenextweb.com/apps/2019/10/07/a-new-study-says-nearly-96-of-deepfake-videos-are-porn/

مقاطع فيديو وصور إباحية مزيفة بعد أن بحثت على نفسها من خلال محرك البحث "Google" الأمر الذي ولّد لديها أضراراً نفسية جسيمة[1]. وفي واقعة أخرى أدت إلى انتحار فتاه مصرية في مُقتبل عمرها (16 عاماً) في يناير 2022 بعدما استغل أحد الأشخاص صورها المتاحة على مواقع التواصل الاجتماعي ليصنع محتوى إباحي مزيف لها ويطلقه ليتداول بين أفراد مدينتها فما وجدت ملاذا لصون شرفها وسمعتها سوى الموت[2].

ثانياً: التكييف القانوني لتقنية التزييف العميق "deepfakes"

ربما يُثار التساؤل حول كُنه تلك التقنية من منظور القانون الجنائي، هل تُعد مجرد وسيلة أو أداة لارتكاب الجريمة، أم أن استعمالها في حد ذاته يُشكل ركناً مادياً لجريمة مستقلة؟

يُفترض في معرض الإجابة على هذا التساؤل الرجوع إلى التشريعات التي تناولت تلك التقنية، لتحديد ما إذا كان استعمالها في حد ذاته يمثل جريمة مستقلة أم أنها مجرد أداة أو وسيلة لتحقيق أغراض إجرامية، فيكون النص الجنائي هو المعيار الحاسم لبيان ذلك. بيد أن التشريعات العربية

---

(1) Ally Foster, Picture Reveals Sickening Online Secret, NEWS.COM.AU (JUNE 30, 2018, 7:33AM), , Available at: https://www.news.com.au/technology/online/security/teens-google-search-reveals-sickening-online-secret-about-herself/news-story/ee9d26010989c4b9a5c6333013ebbef2.

(2) مقال بعنوان: انتحار فتاة الغربية وتفاصيل رسالتها الأخيرة، بوابة الأهرام، على الرابط المرفق، بتاريخ دخول 4/ يناير/ 2022م، الساعة 10:51 صباحاً:
https://gate.ahram.org.eg/News/3237950.aspx

كذلك الأوروبية[1] قد خلت جميعها من مصطلح التزييف العميق "deepfakes" في نصوص القانون الجنائي لديها، على خلاف ذلك سنّت ثلاث ولايات أمريكية فقط، حتى كتابة هذه السطور، تشريعات مختلفة لمكافحة هذه الظاهرة من خلال تلك التقنية الحديثة.

سارعت ولاية فرجينيا بفرض عقوبات جنائية على المواد الإباحية المزيفة من خلال التقنيات المعدّة لذلك والتي من بينها تقنية التزييف العميق بدون موافقة ذوي الشأن وبقصد الإكراه أو المضايقة أو التخويف. ذلك القانون الذي دخل حيز التنفيذ في 1 يوليو 2019، جعل اصطناع أو بيع أو توزيع الصور ومقاطع الفيديو الإباحية المفبركة جنحة من الدرجة الأولى، يُعاقب عليها بالسجن لمدة تصل إلى عام وغرامة قدرها 2500 دولار[2]. وفي

---

(1) Hogan Lovells, Penelope Thornton, Patrick Fromlowitz, Aissatou Sylla, Rachel Shelbourne Fleeson and Margaret (Maggie) Kathryn Pennisi. Deepfakes: An EU and U.S. perspective, July 24 2020, Available at:
https://www.lexology.com/library/detail.aspx?g=8f038b17-a124-46b2-85dc-374f3ccf9392

(2) CHAPTER 490; An Act to amend and reenact § 18.2-386.2 of the Code of Virginia, relating to unlawful dissemination or sale of images of another person; penalty.

Be it enacted by the General Assembly of Virginia:

.1That § 18.2-386.2 of the Code of Virginia is amended and reenacted as follows:

.386.2-18.2 §Unlawful dissemination or sale of images of another; penalty.

A. Any person who, with the intent to coerce, harass, or intimidate, maliciously disseminates or sells any video graphic or still image created by any means whatsoever that depicts another person who is totally nude, or in a state of undress so as to expose the genitals, pubic area, buttocks, or female breast, where such person knows or has reason to know that he is not licensed or authorized to disseminate or sell such video graphic or still image is guilty of a Class 1 misdemeanor. However, if for purposes of this subsection, "another person" includes a person whose image was used in creating, adapting, or modifying a video graphic or still image with the intent to depict an actual person and who is recognizable as an actual person by the person's face, likeness, or other distinguishing characteristic.

B. If a person uses services of an Internet service provider, an electronic mail service provider, or any other information service, system, or access software provider that provides or enables computer access by multiple users to a computer server in committing acts prohibited under this section, such provider shall not be held responsible for violating this section for content provided by another person.

B. C. Venue for a prosecution under this section may lie in the jurisdiction where the unlawful act occurs or where any video graphic or still image created by any means whatsoever is produced, reproduced, found, stored, received, or possessed in violation of this section.

C. D. The provisions of this section shall not preclude prosecution under any other statute.

الأول من سبتمبر 2019، جرّمت 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 قصُد منه "إيذاء مرشح معين أو التأثير على نتيجة الانتخابات" حال "نشرها وتوزيعها خلال 30 يومًا من الانتخابات" واعتبرت هذا الفعل كذلك جنحة من الدرجة الأولى يُعاقب مرتكبها بالسجن لمدة عام في أحد سجون الولاية وغرامة تصل إلى 4000 دولار[1].

النموذجين السالف ذكرهما في ولايتي تكساس وفيرجينيا إنما اعتبرا تقنية التزييف العميق مجرد وسيلة لتحقيق غرض إجرامي متمثل في التأثير

---

[1] S.B. No. 751: AN ACT relating to the creation of a criminal offense for fabricating a deceptive video with intent to influence the outcome of an election.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

SECTION 1. Section 255.004, Election Code, is amended by adding Subsections (d) and (e) to read as follows: (d) A person commits an offense if the person, with intent to injure a candidate or influence the result of an election:

(1) creates a deep fake video; and

(2) causes the deep fake video to be published or distributed within 30 days of an election.

(e) In this section, "deep fake video" means a video created with artificial intelligence that, with the intent to deceive, appears to depict a real person performing an action that did not occur in reality.

SECTION 2. This Act takes effect September 1, 2019.

على أحد المرشحين أو الإخلال بنزاهة العملية الانتخابية في الولاية الأولى[1]، ومتمثل في الانتقام الإباحي العميق في الولاية الثانية.

وفي أكتوبر 2019 أضافت ولاية كاليفورنيا نصوصاً تحظر على أي شخص أو كيان، إنتاج أو توزيع أو نشر أو بث، بسوء نية مواد دعائية انتخابية مزيفة تحتوي على صورة أو صوت لشخص أو أشخاص المرشحين من خلال تقنية التزييف العميق خلال 60 يومًا من الانتخابات[2]، ورغم أنها

---

(1) Matthew Ferraro. Texas Law Could Signal More State, Federal Deepfake Bans, Reprinted with Permission from Law360, Available at:
https://www.jdsupra.com/legalnews/texas-law-could-signal-more-state-37742/

(2) – SECTION. 3. Section 20010 of the Elections Code is amended to read:

20010. (a) Except as provided in subdivision (b), a person, firm, association, corporation, campaign committee, or organization shall not, with actual malice, produce, distribute, publish, or broadcast campaign material that contains (1) a picture or photograph of a person or persons into which the image of a candidate for public office is superimposed or (2) a picture or photograph of a candidate for public office into which the image of another person or persons is superimposed. “Campaign material” includes, but is not limited to, any printed matter, advertisement in a newspaper or other periodical, television commercial, or computer image. For purposes of this section, “actual malice” means the knowledge that the image of a person has been superimposed on a picture or photograph to create a false representation, or a reckless disregard of whether or

not the image of a person has been superimposed on a picture or photograph to create a false representation.

(b) A person, firm, association, corporation, campaign committee, or organization may produce, distribute, publish, or broadcast campaign material that contains a picture or photograph prohibited by subdivision (a) only if each picture or photograph in the campaign material includes the following statement in the same point size type as the largest point size type used elsewhere in the campaign material: "This picture is not an accurate representation of fact." The statement shall be immediately adjacent to each picture or photograph prohibited by subdivision (a).

(c) (1) Any registered voter may seek a temporary restraining order and an injunction prohibiting the publication, distribution, or broadcasting of any campaign material in violation of this section. Upon filing a petition under this section, the plaintiff may obtain a temporary restraining order in accordance with Section 527 of the Code of Civil Procedure.

(2) A candidate for public office whose likeness appears in a picture or photograph prohibited by subdivision (a) may bring a civil action against any person, firm, association, corporation, campaign committee, or organization that produced, distributed, published, or broadcast the picture or photograph prohibited by subdivision (a). The court may award damages in an amount equal to the cost of producing, distributing, publishing, or broadcasting the campaign material that violated this section, in addition to reasonable attorney's fees and costs.

لم تجرم الفعل إلا أنها أعطت الحق للمضرور برفع دعوى قضائية يستحق بموجبها تعويضاً مقابل ما لحقه من ضرر وما فاته من كسب.

باستقراء تلكم التشريعات الثلاثة السابقة يتبدى لنا بجلاء أن تقنية التزييف العميق غير مُجرمة في ذاتها وإنما لغرض إجرامي ما يتقصّده الجاني بمناسبتها، من ثم لا تتعدى في تكييفها القانوني مجرد الوسيلة أو الأداة التي يستعملها الجاني لارتكاب جريمته[1]، ووفقاً للقاعدة العامة فإن المشرع الجنائي لا يعتد بالوسيلة[2]، وإنما بالاعتداء على المصلحة المحمية

(d) (1) This section does not apply to a holder of a license granted pursuant to the federal Communications Act of 1934 (47 U.S.C. Sec. 151 et seq.) in the performance of the functions for which the license is granted.

(2) This section does not apply to the publisher or an employee of a newspaper, magazine, or other periodical that is published on a regular basis for any material published in that newspaper, magazine, or other periodical. For purposes of this subdivision, a "newspaper, magazine, or other periodical that is published on a regular basis" does not include any newspaper, magazine, or other periodical that has as its primary purpose the publication of campaign advertising or communication, as defined by Section 304.

(e) This section shall become operative on January 1, 2023.

[1] د. حورية محمد عبد الرحيم موسى: أثر وسيلة ارتكاب الجريمة على تشديد العقوبة، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2016م، ص2.

[2] والوسيلة هي "كل ما يتوصل به إلى الشيء". ابن منظور: لسان العرب، المجلد السادس، باب الواو، ج53، دار المعارف، الإسكندرية، 4838.

جنائياً أياً كانت وسيلة هذا التعدّي، إلا أن المشرع في حالات استثنائية قد يخرج عن هذا الأصل لمنح الوسيلة التي ارتكبت بها الجريمة دوراً مهماً في تجريم الفعل أو تشديد العقاب عليه، كما لو جعل الوسيلة أحد مكونات الجريمة لا سيما الجرائم المتعلقة بالتأثير على نزاهة العملية الانتخابية أو الانتقام الإباحي من خلال وسيلة التزييف العميق المستحدثة تقنياً، وبالتالي عند مطابقة السلوك الإجرامي للنموذج القانوني المنصوص عليه يتعين أخذ تلك الوسيلة عين الاعتبار لكونها أحد مكونات النموذج القانوني[1] فلا تقوم الجريمة إلا بها[2].

ثالثاً: سِمات الجريمة المُرتكبة عبر التزييف العميق

تتسم الجرائم المرتبكة عبر تقنية التزييف العميق بثلاث سمات وهم أولاً: تتابع النشاط؛ ومفادها أن سلوك هذه الجرائم مركب من فعلين أولهما جمع البيانات ثانيها تزييفها. ثانيا: العلانية؛ ومقتضاها نشر الفيديو المزيف. ثالثا: صعوبة مُساءلة وملاحقة الجناة.

1- تتابع النشاط

تتسم الجرائم المرتكبة عبر التزييف العميق بتتابع النشاط أو الفعل في عنصر السلوك المكون للركن المادي للجريمة حيث لا يتم اصطناع فيديو مزيف إلا بعد جمع ورصد صور ومقاطع فيديو وتسجيلات صوتيه للشخص

---

[1] د. أمال عبد الرحيم عثمان: النموذج القانوني للجريمة، مجلة العلوم القانونية والاقتصادية، العدد 1، السنة 14، 1972، ص216-217.

[2] ويطلق الفقه الجنائي المصري على هذا النوع من الجرائم "الجرائم ذات الوسيلة المقيدة" وهي تختلف عن الوسيلة المطلقة التي لا يعلق القانون أهمية عليها في ارتكاب الجريمة. د. جلال ثروت: نظم القسم الخاص، جرائم الاعتداء على الأشخاص، دار المطبوعات الجامعية، الإسكندرية، الجزء الأول، 1995م، ص140-141.

المجني عليه في مرحلة أولى، ثم في مرحلة ثانية تحريف تلك البيانات والتلاعب بها لإنشاء الفيديو المزيف، الأمر الذي يشير إلى أن مرحلة واحدة فقط قد لا تكفي لوصف السلوك بالمجرّم، فجمع البيانات المباحة كبيانات الفنانين والأشخاص العامة والأشخاص الذين تنازلوا بإرادتهم عن بياناتهم من على شبكة الإنترنت لا يُعد جريمة مستقلة إلا إذا كانت تلك البيانات مؤمّنة ومحمية من ذويها أو متعلقة بمؤسسات الدولة أو بغرض نشرها على وجه ينتهك الخصوصية. كذلك مجرد اصطناع فيديو مزيف لا يمُس الأشخاص كفعل مستقل لا يُعد فعلاً خطيراً يستوجب اتصافه بالمجرّم خاصة لو كانت تلك المقاطع المزيفة لا تمس الأشخاص من الأساس.

من ثم فالنشاطان مجتمعان يمثلان عنصر السلوك في هذا النوع من الجرائم وهما جمع بيانات شخص محدد أولاً، ثم تزييف تلك البيانات على وجه مخالف للحقيقة ثانياً. فالرابطة التي تجمع بينهما رابطة غائية تستهدف معالجة تلك البيانات من خلال خوارزميات معدّة لذلك لإنتاج فيديو يتضمن محتوً لم يتقوّل به المجني عليه بل هو من تلفيق مُنشئ الفيديو. كما أن النشاطان متعاقبين وفقاً للترتيب الزمني فلا يمكن تقديم الثاني على الأول باعتباره أن الأول محلاً للثاني، فالبيانات محل الفيديو المزيف ولا يمكن إنشائه إلا إذا توفرت بيانات عن الشخص المرصود.

ازدواجية النشاط على النحو السالف ربما يُعد سبباً لتحقق التعدد المادي في جرائم التزييف العميق إذا ما لجأ الجاني في معرض إنشاء الفيديو لاختراق أحد الحسابات الشخصية للاستحواذ على بيانات شخص معين بدون وجه حق ثم يضطلع بتزييف تلك البيانات، ليجمع هذا السلوك جرائم الدخول غير المشروع الذي نص عليها المشرع المصري في القانون 175 لسنة

2018 لديه[1] وكذلك جريمة انتهاك خصوصية شخص دون رضاه عن طريق الشبكة المعلوماتية[2]، فضلاً عن الجريمة المرتبطة بالغرض النهائي لإنتاج الفيديو المزيف سواء كانت ابتزاز إلكتروني أو انتقام إباحي أو غيرها من الجرائم.

2- العلانية

لما كان الغرض من إنشاء مقاطع فيديو مزيفة هو الانتقام الإباحي أو الابتزاز الإلكتروني أو التشهير أو التأثير على نزاهة العملية السياسية أو غيرها، فلن يتحقق هذا الغرض إلا إذا تم نشر الفيديو المزيف أو التهديد

---

[1] حيث نصت المادة (١٤) على أنه "يُعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمدًا، أو دخل بخطأ غير عمدي وبقي بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتى محظور الدخول عليه.

فإذا نتج عن ذلك الدخول إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتى، تكون العقوبة الحبس مدة لا تقل عن سنتين، وغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتى ألف جنيه، أو بإحدى هاتين العقوبتين".

[2] وهو ما نصت على المادة 25 من القانون رقم 175 لسنة 2018م بأن "يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من اعتدى على أى من المبادئ أو القيم الأسرية فى المجتمع المصرى، أو انتهك حرمة الحياة الخاصة أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع إلكترونى لترويج السلع أو الخدمات دون موافقته، أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخبارًا أو صورًا وما فى حكمها، تنتهك خصوصية أى شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة".

بنشره، وإلا ما جدوى إنشاءه من الأساس؟ فليس هناك من فائدة تعود على مُنشئ الفيديو المزيف حال اصطناعه وبقائه في حوزته دون أن يُخبر به أحداً، فالعلانية هنا يقصد بها إتاحة الفيديو المزيف للعامة والجمهور من خلال أيٍّ من وسائل النشر التكنولوجية كوسائل التواصل الاجتماعي أو المنصات الرقمية أو المواقع الإلكترونية أو إرساله عبر تطبيقات الهواتف الذكية كالواتس أب أو التليجرام أو غيرها من الوسائل، كما لا يُقصد بالعلانية التزامن أو التعاصر بينها وبين إنشاء الفيديو المزيف بل تتحقق العلانية بالنشر حتى بعد إنتاج الفيديو المزيف ولو في أي وقت لاحق عليه، من ثم فالعلانية تمثل بلا أدنى شك أحد أركان الجريمة التي ترتكب بواسطة تقنية التزييف العميق. غير أن التساؤل الواجب طرحه ما لو تم إظهار المقطع الجنسي الإباحي دون أن يتحقق عنصر العلانية، كما لو أرسل الفيديو للضحية من خلال تراسل إلكتروني خاص فهل يكون مسؤولا جنائيا أم لا؟

جدير بالذكر أن المشرع الجنائي المصري لم يُكرس تجريم الفيديوهات المزيفة بالقدر الذي كرسه للصور أو مقاطع الفيديو العادية فبالنظر إلى المواد 178[1] و178 مكرر ثانياً[2]، نجد أنه قد قصر العقوبة

---

[1] نصت المادة 178 عقوبات مصري على أن "يعاقب بالحبس مدة لا تزيد على سنتين وبغرامة لا تقل عن خمسة آلاف جنيه ولا تزيد على عشرة آلاف جنيه أو بإحدى هاتين العقوبتين كل من نشر أو صنع أو حاز بقصد الاتجار أو التوزيع أو الإيجار أو اللصق أو العرض مطبوعات أو مخطوطات أو رسومات أو إعلانات أو صوراً محفورة أو منقوشة أو رسوماً يدوية أو فوتوغرافية أو إشارات رمزية أو غير ذلك من الأشياء أو الصور عامة إذا كانت خادشه للحياء العام".

[2] نصت المادة 178 مكرر ثانياً عقوبات مصري في فقرتها الأولى على أن "يعاقب بغرامة لا تقل عن عشرة آلاف جنيه ولا تزيد على ثلاثين ألف جنيه كل من نشر أو صنع

على من يضّطلع باصطناع صور غير حقيقية بغرض الاتجار أو التوزيع أو الإيجار أو اللصق أو العرض وإذا كان من شأن تلك الصور الإساءة إلى سمعة البلاد أو إذا كانت بطبيعتها خادشه للحياء العام. أما من حيث مقاطع الفيديو التي جرمها المشرع المصري صراحةً فكانت قاصرة على حالة وحيدة فقط وهي نشر مقاطع فيديو لوقائع جلسة محاكمة مخصصة لنظر دعوى جنائية بدون تصريح من رئيس المحكمة المختصة، وبعد أخذ رأي النيابة العامة وفقاً للمادة 186 مكرر المضافة بالقانون رقم 71 لسنة 2021م[1]، ورغم حداثة هذا التعديل إلا أن المشرع لم يجعل تزييف محتوى تلك المقاطع ظرفاً مشدداً للعقوبة، فإذا كان نشر المحتوى السليم لمقطع الفيديو بغير إذن معاقباً عليه فمن باب أولى أن تُشدد هذه العقوبة إذا تم التلاعب بمحتوى هذه المقاطع وتزييفه.

3- صعوبة مُساءلة وملاحقة الجناة

تكمن صعوبة مساءلة الجناة في تحديد شخص المجرم أولاً، وإسناد الجريمة له ثانياً. لتثور عدة تساؤلات حول تحديد المسؤول جنائياً فهل هو الشخص الذي أنشأ الفيديو الأصلي أم الذي استخدم التزييف العميق أم الذي قام بتحميله على الموقع أم الذي شاركه عبر الإنترنت أم مزود الخدمة الذي

أو حاز بقصد الاتجار أو التوزيع أو الإيجار أو اللصق أو العرض صوراً غير حقيقية من شأنها الإساءة إلى سمعة البلاد".

[1] نصت المادة 186 مكرر عقوبات مصري على إنه "مع عدم الإخلال بأي عقوبة أشد يُعاقب بغرامة لا تقل عن مائة ألف جنيه ولا تزيد على ثلاثمائة ألف جنيه كل من صور أو سجل كلمات أو مقاطع أو بث أو نشر أو عرض بأي طريق من طرق العلانية لوقائع جلسة محاكمة مخصصة لنظر دعوى جنائية بدون تصريح من رئيس المحكمة المختصة، وبعد أخذ رأى النيابة العامة".

علم بالمحتوى غير المشروع؟ لا تثور الإشكالية إذا كان من قام بكافة النشاط هو شخص واحد فيكون هو المسؤول جنائياً، وإنما تدق الإشكالية إذا تعدد الفاعلون في كل مرحلة من المراحل فمن يكون فاعلاً أصلياً ومن يكون شريكاً؟

وتكمن من ناحية أخرى صعوبة الملاحقة الجنائية في ما تتسم به هذه الجريمة من طابع عالمي لا يحتاج تنفيذها التواجد في إقليم محدد وإنما هي عابرة للحدود يتم بثها من خلال الإنترنت وما يتطلبه من تعاون دولي لعدم الإفلات من العقاب.

رابعاً: أهمية البحث

للبحث أهمية موضوعية تكمن في بيان أوجه المعالجة الجنائية الموضوعية للحدِّ من تلك الظاهرة التكنولوجية الحديثة التي تعطي للأفراد العاديين القدرة على الانتقام بالتشهير من خلال فبركة مقاطع الفيديو يصعب اكتشاف تزييفها، تُمثل انتهاكاً للحق في الشرف والاعتبار من ناحية، والحق في الخصوصية من ناحية أخرى. بالإضافة إلى سلبيات إهدار حجية الأدلة الصوتية والمرئية بشكل عام أمام جهات التحقيق أو القضاء الجنائي رغم الاعتراف بحجيتها صراحة في التشريعات المختلفة كما هو في التشريع الجنائي المصري[1].

[1] وهو ما نصت عليه المادة 11 من القانون رقم 175 لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات بأنه "يكون للأدلة المستمدة أو المستخرجة من الأجهزة أو المعدات أو الوسائط أو الدعامات الإلكترونية أو من النظام المعلوماتي أو من برامج الحاسب، أو من أي وسيلة لتقنية المعلومات ذات قيمة وحجية الأدلة المادية في الإثبات الجنائي متى توافرت بها الشروط الفنية الواردة باللائحة التنفيذية لهذا القانون".

للبحث كذلك أهمية إجرائية تتجسد في كيفية تحديد المسؤول جنائياً، نظراً لكثرة المساهمين في هذه الجريمة، ومن منهم فاعلاً أصلياً ومن منهم شريك، فضلاً عن استجلاء آلية الملاحقة القضائية للمجرم المعلوماتي في جريمة الانتقام الإباحي بواسطة التزييف العميق.

خامساً: نطاق البحث

يدور البحث حول جريمة الانتقام الإباحي عبر تقنية التزييف العميق "deepfakes" والمسؤولية الجنائية عنها، من خلال بيان ركنها المادي والمعنوي في النصوص الجنائية لدى المشرع المصري سواء في قانون العقوبات التقليدي أو في قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، كذلك تحديد المسؤول جنائياً عن ارتكاب هذه الجريمة في كل مرحلة من مراحل الركن المادي المكون لها وآليات الملاحقة القضائية له.

سادساً: إشكالية البحث وتساؤلاته

إشكالية البحث تتمثل في تحديد ماهية جريمة الانتقام الإباحي عبر تقنية التزييف العميق والمسؤولية الجنائية الناشئة عنها؟ ويتفرع عن هذه الإشكالية عدة تساؤلات يُجاب عليها، لعلّ أهمها ما يلي؛

1- هل تبنت التشريعات المصرية نصوصاً خاصة بتجريم تقنية إنشاء مقاطع فيديو مزيفة كما فعل المشرع الأمريكي في بعض الولايات؟

2- هل تتميز جريمة الانتقام الإباحي العميق عن جريمة الانتقام الإباحي المجرد أو المحض؟ وكذلك عن جريمة الابتزاز الإلكتروني؟

3- ما هي مراحل السلوك المكون لجريمة التزييف الإباحي العميق؟ وهل تعد كل مرحلة جريمة مستقلة بذاتها؟ وهل يستلزم الركن المعنوي لجرائم التزييف العميق قصداً جنائياً خاصاً أو لا؟

4- من هو المسؤول جنائياً عن جريمة التزييف الإباحي العميق، متصيّد البيانات الشخصية أم معالج تلك البيانات باستخدام تقنية التزييف العميق أم من يقوم بإظهار الفيديو الجنسي المزيف؟

5- في حالة نشر المقطع الجنسي المزيف عن الإنترنت هل تمتد المسؤولية الجنائية لمدير الموقع أو مقدم الخدمة أو متعهد الإيواء أم تقتصر على الناشر فقط؟ وهل إعادة النشر أو الإعجاب بمقطع فيديو مزيف على وسائل التواصل الاجتماعي يعد جريمة مستقلة؟

6- كيف يمكن الملاحقة القضائية لمرتكبي جريمة التزييف الإباحي العميق باعتبارها من الجرائم التي لا تتقيد بنطاق إقليمي معين إذ يتم ارتكابها من خلال الإنترنت؟

سابعاً: منهجية البحث

عمد الباحث إلى تحليل النصوص الجنائية التي تناولت بين طياتها تقنية التزييف العميق لدى المشرع المصري وبعض التشريعات المقارنة، فضلاً عن محاولة تأصيل تلك الجرائم لديه، لذا تكون منهجية البحث تحليلية مقارنة.

ثامناً: خطة البحث

يقسم البحث إلى شق موضوعي وآخر إجرائي، ليتناول أولاً تحديد مفهوم جريمة الانتقام الإباحي عبر تقنية التزييف العميق"Deepfakes"

وتمييزها وأركانها والعقوبة المقررة لها لدى المشرع المصري، وثانياً المسؤولية الجنائية الناشئة عن هذه الجريمة وذلك في مبحثين متتالين؛

المبحث الأول: جريمة الانتقام الإباحي عبر تقنية التزييف العميق"Deepfakes".

المبحث الثاني: المسؤولية الجنائية عن جريمة الانتقام الإباحي عبر تقنية التزييف العميق"Deepfakes".

المبحث الأول

جريمة الانتقام الإباحي عبر تقنية التزييف العميق"Deepfakes"

تمهيد

نُجيب من خلال هذا المبحث على عدة تساؤلات وهي؛ ما المقصود بالانتقام الإباحي العميق، وما يُميزه عن الانتقام الإباحي المجرد، وما الفرق بينه وبين الابتزاز الإلكتروني؟ وما هي أركان هذه الجريمة؟ وهل يشدد العقاب فيها بقدر خطورة الوسيلة التقنية المستحدثة أم لا؟ وهل تستغرق نصوص قانون العقوبات المصري هذه الجريمة أم هي مباحة لحين تدخل المشرع بالنص عليها صراحة؟

أولاً: مفهوم الانتقام الإباحي العميق

الانتقام الإباحي مصطلح مركب من الانتقام وهو الثأر من شخص ما كرد فعل عمّا بدر منه من إيذاء دفع الآخر لإيذائه مادياً أو معنوياً[1]، والإباحي مفاده الكشف عن مواطن العفة لدى الشخص ذاته، من ثم فالانتقام الإباحي يعني نشر صور ومقاطع جنسية لشخص ما كمحاولة لعقابه وإيذاءه[2]. بيد أن هناك جانب نفسي لدى الجاني يدرك من خلاله أن فضح الصور والمقاطع الجنسية دون رضاء من المجني عليه الضحية يشفي غليله،

---

[1] د. أحمد عبد الموجود زكير: جريمة التزييف الإباحي العميق، دراسة مقارنة، المجلة القانونية، جامعة القاهرة، كلية الحقوق (فرع الخرطوم)، المجلد 11، العدد 7، 2022م، ص2229.

[2] وذلك بحسب تعريف قاموس كامبريدج على الرابط التالي، بتاريخ دخول 2022/8/8م، الساعة 1:10

https://dictionary.cambridge.org/dictionary/english/revenge-porn

وغالباً ما يكون هذا السلوك كردة فعل عن انفصال حبيبين أو شريكين سابقين[1]، إلا أن هناك أحوال أخرى لها جانب نفسي مشوه قد تكون هي الدافع لنشر هذه المقاطع الجنسية كوسيلة لطلب الفدية أو الحصول على المال أو لإرضاء شعور غريزي لديه أو إشباع جنسي معين، أو تحقيق مكاسب من خلال رفع تلك المقاطع على موقع إباحي خاص به أو غيرها[2].

أما الانتقام الإباحي العميق يُقصد به بث ومشاركة لمقاطع فيديو جنسية تم إنتاجها وتوليدها من خلال تقنية التزييف العميق"Deepfakes" بغير رضا من المجني عليه ذكراً كان أو أنثى وبغرض الانتقام منه[3]، وهذا النوع من الانتقام يختلف بطبيعته عن الانتقام الإباحي المجرد الذي سبق ذكره، والذي ينضوي على مجرد إفشاء سرية مقاطع جنسية وبثّها دون رغبه المجني عليه في ذلك[4]، فالنوع الأخير الواقعة الإباحية فيه حقيقة ورضائية

---

(1) Franks (M.-A.), The Crime of "Revenge Porn", In: Alexander (L.), Ferzan (K.-K.)(eds.), The Palgrave Handbook of Applied Ethics and the Criminal Law, Palgrave Macmillan, 2019, p.663.

(2) Flynn (A.) & Henry (N.), Image-Based Sexual Abuse: An Australian Reflection, Women & Criminal Justice, 2019, pp.2 et s.

(3) Edvinas Meskys, Julija Kalpokiene, Paulius Jurcys, Aidas Liaudanskas; Regulating Deep Fakes: Legal and Ethical Considerationsm Journal of Intellectual Property Law & Practice, Volume 15, Issue 1, January 2020, P.7.

(4) ولعل هذا النوع من الانتقام هو ما تعرض له "بنجامان غريفو" الوزير السابق في الحكومة الفرنسية وعضو حزب "الجمهورية إلى الأمام" الحاكم، حال خوضه لانتخابات رئاسة بلدية باريس عام 2020 مما دفعه على الانسحاب من سباق تلك الانتخابات، يرجع في ذلك إلى الموقع التالي، بتاريخ دخول 6/ أغسطس/ 2022م، الساعة 3:40م:

كل ما هناك أنها كانت سرية ثم أعلنت وانتشرت بغير رضا صاحبها بغرض الانتقام منه. أما النوع الأول الواقعة الإباحية فيه مزيفة وملفقة بالكامل وهو ما يجعل الانتقام الإباحي العميق أشد ضراوة وخطورة عن نظيره المجرد أو المحض، إذ أن المجني عليه فيها لم يرتكب هذه الأفعال من الأصل وإنما استخدمت صوره وصوته وحركاته وتعبيراته لإنتاج المقطع الجنسي على نحو مخالف للحقيقة.

بيد أن الانتقام الإباحي المحض أو المجرد يكون دائماً لاحق على أحد الأمرين إما بمناسبة علاقة حميمية سابقة برضاء طرفيها سواء كانت مشروعة أو غير مشروعة من خلال نشر صور أو مقاطع فيديو مسجلة دون علم الطرف الآخر بها، أو باستهداف بيانات شخص ما من خلال اختراق هاتفه المحمول أو جهازه الحوسبي أو بريده الإلكتروني لسرقة مقاطع الفيديو الإباحية ثم نشرها على الإنترنت. جدير بالذكر أن في الآونة الأخيرة، هناك 48 ولاية أمريكية لديها قوانين لمكافحة الانتقام الإباحي المجرد[1]. وتختلف درجات الحماية بين ولاية لأخرى فعلى سبيل المثال تُصنف بعض الولايات تلك الجريمة على أنها جنحة يعاقب عليها بالسجن لمدة تصل إلى عام كحد

---

https://www.leparisien.fr/elections/municipales/direct-retrait-de-benjamin-griveaux-a-paris-reunion-de-crise-chez-lrem-a-14-heures-14-02-2020-8259573.php

[1] Sales (J.) & Magaldi (J.), "Deconstructing the Statutory Landscape of "Revenge Porn": An Evaluation of the Elements That Make an Effective Nonconsensual Pornography Statute", American Criminal Law Review, Vol. 57(4), 2020, p.1505.

أقصى في سجن المقاطعة مثل ولاية كونيتيكت "Connecticut"[1]، ويصنفها البعض الآخر على أنها جناية مثل ولاية نيو هامبشاير" New

---

[1] Connecticut General Statutes Title 53A. Penal Code § 53a-189c. (a) A person is guilty of unlawful dissemination of an intimate image when (1) such person intentionally disseminates by electronic or other means a photograph, film, videotape or other recorded image of (A) the genitals, pubic area or buttocks of another person with less than a fully opaque covering of such body part, or the breast of such other person who is female with less than a fully opaque covering of any portion of such breast below the top of the nipple, or (B) another person engaged in sexual intercourse, as defined in section 53a-193, (2) such person disseminates such image without the consent of such other person, knowing that such other person understood that the image would not be so disseminated, and (3) such other person suffers harm as a result of such dissemination. For purposes of this subsection, “disseminate” means to sell, give, provide, lend, trade, mail, deliver, transfer, publish, distribute, circulate, present, exhibit, advertise or otherwise offer.

(b) The provisions of subsection (a) of this subsection shall not apply to:

(1)Any image described in subsection (a) of this section of such other person if such image resulted from voluntary exposure or engagement in sexual intercourse by such other person, in a public place, as defined in section 53a-181 , or in a commercial setting;

Hampshire"[1] فيعاقب عليها بالسجن لأكثر من عام[1]، غير أنه ليس هناك قانون فيدرالي أمريكي يسري على كافة الولايات يجرم هذا السلوك حتى كتابة هذه السطور.

---

(2)Any image described in subsection (a) of this section of such other person, if such other person is not clearly identifiable; or

(3)Any image described in subsection (a) of this section of such other person, if the dissemination of such image serves the public interest.

(c) Unlawful dissemination of an intimate image is a class A misdemeanor.

(d) Nothing in this section shall be construed to impose liability on the provider of an interactive computer service, as defined in 47 USC 230, an information service, as defined in 47 USC 153, or a telecommunications service, as defined in section 16-247a, for content provided by another person.

[1] **644:9 Violation of Privacy. –** I. A person is guilty of a class A misdemeanor if such person unlawfully and without the consent of the persons entitled to privacy therein, installs or uses:

(a) Any device for the purpose of observing, photographing, recording, amplifying, broadcasting, or in any way transmitting images or sounds of the private body parts of a person including the genitalia, buttocks, or female breasts, or a person's body underneath that person's clothing; or

(b) In any private place, any device for the purpose of observing, photographing, recording, amplifying or broadcasting, or in any way transmitting images or sounds in such place; or

(c) Outside a private place, any device for the purpose of hearing, recording, amplifying, broadcasting, observing, or in any way transmitting images, location, movement, or sounds originating in such place which would not ordinarily be audible, visible, or comprehensible outside such place.

II. As used in this section, "private place" means a place where one may reasonably expect to be safe from surveillance including public restrooms, locker rooms, the interior of one's dwelling place, or any place where a person's private body parts including genitalia, buttocks, or female breasts may be exposed.

III. A person is guilty of a class A misdemeanor if that person knowingly disseminates or causes the dissemination of any photograph or video recording of himself or herself engaging in sexual activity with another person without the express consent of the other person or persons who appear in the photograph or videotape. In this paragraph, "disseminate" and "sexual activity" shall have the same meaning as in RSA 649-A:2.

III-a. A person is guilty of a misdemeanor if, for the purpose of arousing or gratifying the person's sexual desire, he or she knowingly views another person, without that person's knowledge or consent, in a place where one would have a reasonable expectation of privacy. For purposes of this paragraph, "views" means looking at another person with the unaided eye or any device intended to improve visual acuity.

IV. A person is guilty of a misdemeanor if such person knowingly enters any residential curtilage, as defined in RSA 627:9, I, or any other private place as defined in paragraph II of this section,

وفي فرنسا عاقب المشرع على الانتقام الإباحي المجرد بموجب المادة 226-1 من قانون العقوبات المعدلة في 2020م[2] من خلال تسجيل

---

without lawful authority and looks into the residential structure thereon or other private place with no legitimate purpose. V. Paragraphs I and II shall not be construed to impair or limit any otherwise lawful activities of law enforcement personnel, nor are paragraphs I and II intended to limit employees of governmental agencies or other entities, public or private, who, in the course and scope of their employment and supported by articulable suspicion, attempt to capture any type of visual image, sound recording, or other physical impression of a person during an investigation, surveillance, or monitoring of conduct to obtain evidence of suspected illegal activity, the suspected violation of any administrative rule or regulation, a suspected fraudulent insurance claim, or any other suspected fraudulent conduct or activity involving a violation of law, or pattern of business practices adversely affecting the public health or safety.

Source. 1971, 518:1. 1995, 280:9. 2003, 256:1. 2004, 212:1, 2. 2005, 264:1. 2008, 334:7. 2012, 76:1, eff. Jan. 1, 2013.

(1) Ruobing Su, Tom Porter, and Michelle Mark: Here's a map showing which US states have passed laws against revenge porn — and those where it's still legal, Available at: https://www.businessinsider.com/map-states-where-revenge-porn-banned-2019-10

(2) Art 226-1; Modifié par LOI n°2020-936 du 30 juillet 2020 - art. 17; Est puni d'un an d'emprisonnement et de 45 000 euros

الصوت أو التقاط صور أو تثبيت كاميرا مراقبة لتسجيل مقاطع جنسية دون علم أو رغبة الطرف الآخر، كما عاقب المشرع الفرنسي على جريمة نشر هذا المحتوى الجنسي بدون موافقة صاحبها ذكراً كان أم أنثى وهو ما نصت

---

d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui:

1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel ;

2° En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.

3° En captant, enregistrant ou transmettant, par quelque moyen que ce soit, la localisation en temps réel ou en différé d'une personne sans le consentement de celle-ci.

Lorsque les actes mentionnés aux 1° et 2° du présent article ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé.

Lorsque les actes mentionnés au présent article ont été accomplis sur la personne d'un mineur, le consentement doit émaner des titulaires de l'autorité parentale.

Lorsque les faits sont commis par le conjoint ou le concubin de la victime ou le partenaire lié à la victime par un pacte civil de solidarité, les peines sont portées à deux ans d'emprisonnement et à 60 000 euros d'amende.

عليه المادة 226-2 التي أدخلت على قانون العقوبات في عام 2016[1]، حتى ولو كان الطرف المعنى وافق على المحتوى الجنسي إلا ان نشره يظل مجرم طالما لم يبد رغبته بالموافقة على نشره صراحة وفقاً لما نصت عليه المادة 226-2-1[2].

بناء عليه فالانتقام الإباحي المجرد يستوي فيه أن يكون الطرفان على علم بأن هناك كاميرا مثبته في مكان خاص تقوم بتسجيل العلاقة الحميمية أو

---

[1] Art 226-2 ; Est puni des mêmes peines le fait de conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser de quelque manière que ce soit tout enregistrement ou document obtenu à l'aide de l'un des actes prévus par l'article 226-1.

Lorsque le délit prévu par l'alinéa précédent est commis par la voie de la presse écrite ou audiovisuelle, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables.

[2]Art 226-2-1 ; Lorsque les délits prévus aux articles 226-1 et 226-2 portent sur des paroles ou des images présentant un caractère sexuel prises dans un lieu public ou privé, les peines sont portées à deux ans d'emprisonnement et à 60 000 € d'amende.

Est puni des mêmes peines le fait, en l'absence d'accord de la personne pour la diffusion, de porter à la connaissance du public ou d'un tiers tout enregistrement ou tout document portant sur des paroles ou des images présentant un caractère sexuel, obtenu, avec le consentement exprès ou présumé de la personne ou par elle-même, à l'aide de l'un des actes prévus à l'article 226-1.

مواطن العفّة عند الرجال أو النساء أو لم يعلم أحدهما بذلك، إذ يستهدف القانون الأمريكي والفرنسي بصفة عامة الحماية الجنائية للحرية الجنسية للمجني عليه وعدم الاعتداء على حقه في الخصوصية لذا فالعقاب منصباً على نشر أو بث أو المراقبة أو التسجيل أو التصوير بغير إذن وموافقة صريحة للشخص المعني برضاء غير معيب أياً كانت صورة الموافقة سواء كتابية أو مسجلة أو غيرها.

من ثم فمناط الاختلاف بين الانتقام الإباحي العميق، ونظيره المجرد يكمن في اتساع نطاق الخطورة الإجرامية وجسامة سلوك الأول عن الثاني، فالاضطلاع بسحب بيانات شخص ما ومعالجتها تقنياً من خلال برامج الذكاء الاصطناعي لإنتاج مقطع جنسي مزيف بالكامل هو بطبيعة الحال فعل أشد خطورة وأكثر جسامة لما ينتابه من كذب وتلفيق واصطناع مناف للحقيقة. فبجانب ضرورة العقاب على فعل فض سرية المقاطع الإباحية بدون علم صاحبها بغرض الانتقام منه وهو ما يتحقق في جريمة الانتقام الإباحي المحض، فالعقاب كذلك ضروري لعملية التلفيق والكذب والتزييف واصطناع مقطع لا وجود له من الأساس على الأقل كظرف مشدد للجريمة.

ثانياً: التمييز بين الانتقام الإباحي العميق والابتزاز الإلكتروني

الابتزاز الإلكتروني يقصد به "كل تهديد يأتيه الجاني، ويؤثر في نفسية المجني عليه أو شخص عزيز لديه، ويتم عبر وسيلة إلكترونية، ويدفعه إلى القيام بما طلبه الجاني أو كلفه به سواء أكان مشروعاً أم غير مشروع"[1] ويتخذ السلوك الإجرامي في جريمة الابتزاز الإلكتروني شكلاً محدداً هو

[1] د. تامر محمد صالح: الابتزاز الإلكتروني، دراسة تحليلية مقارنة، دار الفكر والقانون، المنصورة، 2021م، ص40.

التهديد بإيذاء مقترناً بطلب[1]، ومن ثم فإن التهديد غير المقترن بطلب لا يعد ابتزازاً[2]، وأن يكون مضمون ذلك التهديد إيذاء، إضافة إلى ضرورة أن يكون من شأن هذا التهديد التأثير النفسي على المجني عليه والضغط على إرادته، وأن يكون الجاني قاصداً ذلك، وتتجه إرادته إلى غاية معينة تتمثل في الحصول على المطلوب بناء على ذلك التأثير.

وعرف القانون الأمريكي[3] الابتزاز بموجب المادة 11.417 من The Code of Federal Regulations CFR بأنه: "تعمد توجيه

---

(1) Maeve Maddox, The Difference Between Extortion and Blackmail, Available on: site https://www.dailywritingtips.com/extortion-and-blackmail/ visited on: 1-1-2018.

(2) C.A. Paris, 11° chambre, 25 mai 1999.

(3) وقد حدد الغرض من التهديد وهو الحصول على أموال؛ حيث تنص المادة 875 من قانون العقوبات والإجراءات الجنائية الأمريكي 18 u.s. crimes and criminal code procedure في الفصل 41 من الباب الأول منه والمتعلق بالابتزاز والتهديد على أن:

أ- كل من يرسل أي رسالة تحتوي على طلب للحصول على فدية أو مكافأة لإطلاق سراح أي شخص مختطف، يجب تغريمه بموجب هذا القانون أو السجن لمدة لا تتجاوز عشرين عاماً أو كليهما.

ب- كل من قام، بقصد ابتزاز أي شخص أو شركة أو جمعية أو مؤسسة، للحصول على أموال أو أي شيء آخر ذي قيمة، عن طريق تهديده بالخطف، أو الإصابة، يتم تغريمه بموجب هذا القانون أو السجن لمدة لا تزيد عن عشرين عاماً أو كليهما.

اتهامات كاذبة ضد شخص آخر بأي وسيلة، للحصول أو محاولة الحصول على أي أموال أو سلع أو ممتلكات أو أي شيء آخر ذي قيمة"[1].

وفي فرنسا عرّفت المادة ٣١٢-١ من قانون العقوبات الابتزاز بأنه: "فعل الحصول على الشيء بالعنف أو التهديد بالعنف أو الإكراه للتوقيع أو

ج- كل من يرسل رسالة تنطوي على أي تهديد بخطف أي شخص أو تهديده بإصابة شخص آخر، يتم تغريمه بموجب هذا القانون أو السجن لمدة لا تزيد عن خمس سنوات أو كليهما.

د- كل من قام، بقصد ابتزاز أي شخص أو شركة أو جمعية أو مؤسسة، للحصول على أموال، أو أي شيء آخر ذي قيمة، عن طريق أي اتصال يتضمن تهديداً بإتلاف الممتلكات أو سمعة المرسل إليه، أو أي شخص آخر أو سمعة شخص متوف أو أي تهديد لاتهام المرسل إليه أو أي شخص آخر بجريمة، يتم تغريمه بموجب هذا القانون أو السجن لمدة لا تزيد عن سنتين أو كليهما.

The Code of Laws of the United States of America [1] (variously abbreviated to Code of Laws of the United States, United States Code, U.S. Code, U.S.C., or USC) is the official compilation and codification of the general and permanent federal statutes of the United States. It contains 53 titles (Titles 1–54, excepting Title 53, it being reserved). [2] [3] The main edition is published every six years by the Office of the Law Revision Counsel of the House of Representatives, and cumulative supplements are published annually. [4] [5] The official version of those laws not codified in the United States Code can be found in United States Statutes at Large, Available on: https://en.wikipedia.org/wiki/United States Code site visited on: 1-1-2018.

[1] CFR (Title 25) Chapter I(Subchapter B) Part 11) Subpart D(Section 11.417.

التعهد أو التخلي أو الكشف عن سر أو تحويل أموال أو أوراق مالية أو أي سلعة أخرى"[1].

أما المشرع المصري رغم إصداره لقانون تقنية المعلومات رقم 175 لسنة ٢٠١٨م، غير أنه لم ينص على تجريم الابتزاز الإلكتروني صراحة بصورة مباشرة وشاملة؛ حيث اقتربت من تجريمه على استحياء المادة ٢٥ من القانون المذكور[2] وبخاصة عندما يتعارض الطلب الذي يطلبه الجاني مع المبادئ والقيم الأسرية للمجتمع المصري.

من ثم فالابتزاز الإلكتروني يختلف عن الانتقام الإباحي العميق من حيث ركنه المادي تارة ومن حيث الغرض من إتيان الجريمة تارة أخرى، ومن

---

[1] Art 312-1; L'extorsion est le fait d'obtenir par violence, menace de violences ou contrainte soit une signature, un engagement ou une renonciation, soit la révélation d'un secret, soit la remise de fonds, de valeurs ou d'un bien quelconque.

L'extorsion est punie de sept ans d'emprisonnement et de 100 000 euros d'amende.

[2] والتي نصت على أن: "يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين كل من اعتدى على أي من المبادئ أو القيم الأسرية في المجتمع المصري أو انتهك حرمة الحياة الخاصة، أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع إلكتروني لترويج السلع أو الخدمات دون موافقته، أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات. معلومات أو أخباراً أو صوراً وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة".

حيث الوسيلة تارة ثالثة، فالركن المادي للابتزاز الإلكتروني مناطه التهديد[1] وهو مرحلة سابقة على النشر أو مشاركة أو توزيع المحتوى، على خلاف الانتقام الإباحي العميق الذي يُعد البث أو النشر للمقاطع الإباحية المفبركة هو السلوك المتمم للركن المادي فيه، أما من حيث الغرض من الجريمة دائما ما يكون الابتزاز الإلكتروني مصحوباً بطلب حيث إنها لا تقع كاملة وتامة إلا بقيام المجني عليه بتنفيذ المطلوب منه، أو الامتناع عنه، على خلاف جريمة الانتقام الإباحي التي يتحقق الضرر فيها بمجرد النشر أو البث أو المشاركة أو التراسل للمقاطع الإباحية المزيفة. أما من حيث الوسيلة، فالتهديد محل الابتزاز الإلكتروني يقع بأي وسيلة شفهية كانت أو كتابية أو من خلال وسائط أخرى، أما التزييف الإباحي العميق لا يتحقق إلا بوسيلة واحدة وهي باستخدام تطبيقات الذكاء الاصطناعي المعدّة لذلك، فبدون هذه الوسيلة تنتفي هذه الجريمة فالوسيلة عنصر أساسي في النموذج القانوني لها بخلاف الابتزاز الإلكتروني.

يشترط في التهديد الذي تقع به جريمة الابتزاز الإلكتروني أن يكون بالإيذاء، والأخير قد يكون مادياً أو معنوياً، يتمثل محله في النفس، أو المال، أو السمعة، مما يشكل عدواناً على حياة الإنسان، وخصوصيته، وحريته، وكرامته وسمعته، وملكيته، أما جريمة الانتقام الإباحي العميق الغرض منها هو الانتقام والثأر وتشويه سمعة المجني عليه. كما أن محل الابتزاز الإلكتروني لا يتقيد بالطابع الجنسي كما هو في جريمة الانتقام الإباحي العميق فالإباحية عنصر رئيسي فيها، أما الابتزاز الإلكتروني قد يكون بسبب

---

[1] وهو ما نصت عليه الفقرة الثانية من المادة 327 من قانون العقوبات المصري بقولها "..... ويعاقب بالحبس إذا لم يكن التهديد مصحوباً بطلب أو بتكليف بأمر...."

محتوى غير جنسي كقيام رجل بتهديد آخر بإيقاع أذى به ما لم يساعده في الحصول على إصدار ترخيص قانوني[1].

الضحية في جريمة الابتزاز الإلكتروني يكون مخيراً بين ضررين، فله مُكنة أن يُفاضل بينهما، إما أن يذعن لطلب الجاني حتى لا يقوم بنشر المحتوى، وإما ألا يكترث له باعتبار أن الضرر المتحصل من النشر أخف وطأة مما طلبه الجاني، أما المجني عليه في جريمة الانتقام الإباحي العميق غير مخير بل ربما لا يعلم بأن هناك فيديو مزيف مفبرك تم نشره لغرض الانتقام منه.

التباين بين الجريمتين لا يعني أنهما لا يتكاملان سوياً ليشكل الفعلين نوعاً من أنواع التعدد المادي للجرائم، كمن يضطلع بتزييف مقطع جنسي بغرض الانتقام من شخص ثم يقوم بنشره وحذفه مباشرةً تمهيداً لابتزاز هذا الشخص وأنه قادر على النشر في أي وقت إذا لم يستجب الضحية لطلباته.

ثالثاً: أركان جريمة الانتقام الإباحي العميق

للجريمة وفقاً للقواعد العامة ركن مادي وآخر معنوي، الركن المادي قوامه النشاط المكون للجريمة، سواء كان فعلاً إيجابياً أم مجرد امتناع في الحالات التي يعتبر فيها الامتناع معاقباً عليه وبالشروط اللازمة لذلك. ولابد أن يفضي هذا النشاط إلى النتيجة المحظورة قانوناً، وأن يقوم بين النشاط والنتيجة صلة السببية. أما الركن المعنوي للجريمة قوامه الإرادة والعلم: إرادة

---

[1] د. تامر محمد صالح: الابتزاز الإلكتروني، دراسة تحليلية مقارنة، المرجع السابق، ص22.

السلوك والنتيجة معا (نية تحقيق النتيجة)، والعلم بصلاحية السلوك لإحداث النتيجة وكذا العلم بالعناصر الواقعية الجوهرية اللازمة لقيام الجريمة[1].

1- الركن المادي

غني عن البيان أن الركن المادي له ثلاثة عناصر، وهم السلوك والنتيجة وبينهما رابطة السببية، غير أن عنصر السلوك في الركن المادي في جريمة الانتقام الإباحي العميق متتابع الأفعال بطبيعته[2]، ويمر بمراحل ربما تكون كل مرحلة فيه جريمة مستقلة بذاتها أو شروعاً في جريمة، فحتى يتم تنفيذ النشاط المكون للركن المادي لجريمة الانتقام الإباحي العميق يتطلب من الجاني أولاً أن يضطلع بسحب وتجميع[3] البيانات الشخصية[1] للضحية من

---

[1] د. سليمان عبد المنعم: النظرية العامة لقانون العقوبات، دار المطبوعات الجامعية، الإسكندرية، 2014، ص34.

[2] يقصد بالجريمة متتابعة الأفعال: تلك التي تتمثل في أفعال متعددة، يجمع بينها رغم تعددها تماثل الحق المعتدى عليه، ووحدة الغرض الإجرامي. والجريمة متتابعة الأفعال تتكون إذن من عدة أفعال مستقلة، يصلح كل منها لإقامة جريمة مستقلة، إذ يأتلف كل فعل من ركن مادي وركن معنوي؛ لكنها تصبح رغم ذلك جريمة واحدة وليس عدة جرائم تغليباً لتماثل الحق المعتدى عليه في كل هذه الأفعال "الجرائم"؛ ولوحدة الغرض الإجرامي الذي يجعل من هذه الأفعال وإن تعددت فهي ثمرة لمشروع إجرامي واحد. ولا يطبق على الجريمة المتتابعة سوى عقوبة واحدة. وتشترط محكمة النقض المصرية لقيام الجريمة متتابعة (أو متلاحق) الأفعال أن يكون بين الأزمنة التي ترتكب فيها هذه الأفعال نوع من التقارب حتى يناسب حملها على أنها جميعاً تكون جريمة واحدة. نقض جنائي 9 نوفمبر ١٩٩٤، مجموعة أحكام النقض، س45، ق152، ص983. كذلك د. سليمان عبد المنعم: النظرية العامة لقانون العقوبات، المرجع السابق، ص225.

[3] وقد نصت المادة 2 من القانون رقم ١٥١ لسنة ٢٠٢٠ المصري على أنه "لا يجوز جمع البيانات الشخصية أو معالجتها أو الإفصاح عنها أو إفشائها بأي وسيلة من الوسائل إلا بموافقة صريحة من الشخص المعني بالبيانات، أو في الأحوال المصرح بها قانونًا".

صور وتسجيلات صوتية وفيديوهات سابقة أياً كان مصدرها[2]، غير أن تجميع هذه البيانات أضحى يسيراً بالتزامن مع اتساع نطاق مستخدمي وسائل

وقد عاقب على الإخلال بأحكام هذه المادة بغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مليون جنيه، كل حائز أو متحكم أو معالج امتنع دون مقتض من القانون عن تمكين الشخص المعني بالبيانات من ممارسة حقوقه كما عاقب بغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه كل من جمع بيانات شخصية بدون توافر الشروط المنصوص عليها في المادة (٣) من هذا القانون وهي:

١ – أن تجمع البيانات الشخصية لأغراض مشروعة ومحددة ومعلنة للشخص المعني.

٢ – أن تكون صحيحة وسليمة ومؤمنة.

٣ – أن تعالج بطريقة مشروعة وملائمة للأغراض التي تم تجميعها من أجلها.

٤ – ألا يتم الاحتفاظ بها لمدة أطول من المدة اللازمة للوفاء بالغرض المحدد لها.

وتحدد اللائحة التنفيذية لهذا القانون السياسات والإجراءات والضوابط والمعايير القياسية للجمع والمعالجة والحفظ والتأمين لهذه البيانات. غير أن المخاطبين بهذه العقوبات كل شخص مسؤول عن معالجة البيانات الشخصية سواء كان حائز أو متحكم أو معالج في غير الأحوال المرخص بها قانوناً، وتقع كذلك في الأحوال التي تتم فيها معالجة البيانات بعد الغاء الترخيص الممنوح بالمعالجة أو عند انتهاء مدته كشركات الاتصالات وغيرها.

[1] وقد عرف القانون رقم ١٥١ لسنة ٢٠٢٠ المصري، البيانات الشخصية بأنها: أي بيانات متعلقة بشخص طبيعي محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخرى كالاسم، أو الصوت، أو الصورة، أو رقم تعريفي، أو محدد للهوية عبر الإنترنت، أو أي بيانات تحدد الهوية النفسية، أو الصحية، أو الاقتصادية، أو الثقافية، أو الاجتماعية".

[2] جدير بالذكر أن مصادر استجلاب البيانات محل برامج التزييف العميق متنوعة وآخذة في التنامي لاسيما مع استعمال الهواتف الذكية اللوحية واستخدام التخزين السحابي للبيانات وهي معرضة للاختراق كذلك استخدام البرامج المخصصة لسحب البيانات من قبل متخصصين، أضف إلى ذلك ظاهرة التراسل الجنسي والتي يشارك فيها الأشخاص بمحض إرادتهم للصور والصوتيات والفيديوهات الجنسية، فضلاً عن انتشار الصور الذاتية

التواصل الاجتماعي وتطبيقات الهاتف المحمول لاسيما "واتس أب وانستجرام والتليجرام وتيك توك" وغيرها من التطبيقات[1]. والبيانات الشخصية نوعان إما أن تكون متاحة وهي تلك البيانات التي تنازل صاحبها طواعية عن خصوصيتها بوضعها على وسائل التواصل أمام الجميع. وإما أن تكون هذا البيانات مُشفرة ومحميّة كتلك البيانات المرفوعة على الحوسبات السحابية أو على الإيميل الخاص أو أجهزة الكمبيوتر أو الهاتف اللوحي أو في بنوك المعلومات[2]، هذه البيانات لم يرغب صاحبها في تركها للعامة وإنما اتجهت

التي ترفق على وسائل التواصل الاجتماعي بغرض المشاركة مع الأخرين والتي تمكن الغير من الاطلاع عليها وإساءة استعمالها إذ تبين أن 80% ممن كانوا ضحايا للانتقام الإباحي التقطوا صورهم الجنسية بنفسهم وتراسلوها مع الآخرين.

Hall (M.) and Hearn (J.), «Revenge pornography: gender, sexuality and motivations», Routledge, 2018, p.27; Martinez (C.), An argument for states to outlaw „revenge porn" and for congress to amend 47 U.S.C. §230: how our current laws do little to protect victims, Pittsburgh Journal of Technology Law & Policy, vol. 14 (2), 2014, p. 242.

[1] بلغ عدد مستخدمي وسائل التواصل الاجتماعي في 2022 إلى4.2 مليار مستخدم نشط بحسب التقرير العام الرقمي العالمي لعام على الرابط التالي، بتاريخ دخول 2022/8/10، الساعة 9:30م

https://datareportal.com/reports/digital-2021-global-overview-report

[2] وتعد البنوك وشركات الاتصالات والهيئات الحكومية كهيئة البريد والصحة والسجل المدني أهم أمثلة لبنوك المعلومات، جدير بالذكر أن تجميع هذا النوع من البيانات جريمة عاقب المشرع المصري عليها الأشخاص ممن لهم سيطرة على البيانات الفعلية بحكم عملهم كالمتحكم أو المعالج أو الحائز حال إفشاء أو إتاحة أو تداول أي بيانات شخصية

نيته لإضفاء الخصوصية عليها من خلال وجودها في أماكن لا يجوز التسلل لها من غير كلمة سر لا يعلمها إلا هو(بيانات المرور)، فالتقاط هذه البيانات أصبح غير متاح إلا إذا اخترق الجاني هذه الحماية وهو ما يشكل في حد ذاته سلوكاً لجريمة الدخول غير المشروع لحساب خاص أو نظام معلوماتي تلك الجريمة المعاقب عليها كجريمة مستقلة في مصر[1]، وفرنسا[2]، والولايات المتحدة الأمريكية[1].

معالجة إلكترونياً وشدد العقاب إذا كان القصد من ذلك تعريض الشخص المعني بالبيانات للخطر أو الضرر وفق ما نصت عليه المادة 36 من قانون حماية البيانات الشخصية المصري لعام 2020 والتي نصت على أن "يعاقب بغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مليون جنيه كل حائز أو متحكم أو معالج جمع أو عالج أو أفشي أو أتاح أو تداول بيانات شخصية معالجة إلكترونيًا بأي وسيلة من الوسائل في غير الأحوال المصرح بها قانونًا أو بدون موافقة الشخص المعني بالبيانات".

وتكون العقوبة الحبس مدة لا تقل عن ستة شهور وبغرامة لا تقل عن مائتي ألف جنيه ولا تجاوز مليوني جنيه، أو بإحدى هاتين العقوبتين، إذا ارتكب ذلك مقابل الحصول على منفعة مادية أو أدبية، أو بقصد تعريض الشخص المعني بالبيانات للخطر أو الضرر.

[1] نصت المادة (١٤) من القانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات، الموسومة بـ "جريمة الدخول غير المشروع" على أن "يُعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمدًا، أو دخل بخطأ غير عمدي وبقي بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتي محظور الدخول عليه.

فإذا نتج عن ذلك الدخول إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتى، تكون العقوبة الحبس مدة لا تقل عن سنتين، وغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتى ألف جنيه، أو بإحدى هاتين العقوبتين".

[2] Art 323-1;Modifié par LOI n°2015-912 du 24 juillet 2015 - art. 4; Le fait d'accéder ou de se maintenir, frauduleusement, dans tout

أما المرحلة الثانية من مراحل السلوك المكون للركن المادي لجريمة الانتقام الإباحي العميق هي مرحلة اصطناع مقطع الفيديو من خلال معالجة البيانات التي تم جمعها سلفاً بواسطة معادلات (Formulas)،

---

ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende.

Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 € d'amende.

Lorsque les infractions prévues aux deux premiers alinéas ont été commises à l'encontre d'un système de traitement automatisé de données à caractère personnel mis en œuvre par l'Etat, la peine est portée à cinq ans d'emprisonnement et à 150 000 € d'amende.

(1) 18 U.S. Code § 1030 - Fraud and related activity in connection with computers; (a) Whoever- .....

(7)with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any-

(A) .....;

(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

(C) .....

وخوارزميات[1](Algorithms) الذكاء الاصطناعي[2]، التي تضطلع بتركيب مئات الصور والصوت ومقاطع الفيديو لتوليد وإنتاج المقطع الإباحي المزيف للمجني عليه يصعب بمكان اكتشاف تزييفه. وهذا هو الجانب الأشد خطورة إذ يعطي فيها الجاني لنفسه الحق في التلاعب ببيانات الضحية ليجعله بطلاً في مقطع إباحي في ظل تشريعات جنائية لم يكن في حسبانها تجريم هذا الفعل ومن ثم **يثور التساؤل حول مشروعية هذا الإجراء مستقلاً، هل يعد جريمة تامة في حد ذاته أم شروعا فيها أم عملاً تحضيرياً؟**

في الإجابة على التساؤل الأول فإن حقيقة الأمر ليس هناك نصاً سواء في مصر أو الولايات المتحدة الأمريكية أو فرنسا[3]، يجرم الاستعمال

---

[1] كلمة خوارزمية مستقاة من اسم عالم الرياضيات الفارسي محمد بن موسى الخوارزمي في القرن التاسع وهي باللغة اللاتينية "Algoritmi"، والخوارزمية مدلول مفاده التسلسل الدقيق للخطوات المطلوبة للوصول لشيء معين، والتي يكمن استخدامها للتصنيف، والتحليل، والتنبؤ. د. عبد الله موسي، د. أحمد حبيب بلال: الذكاء الاصطناعي، ثورة في تقنيات العصر، المجموعة العربية للتدريب والنشر، القاهرة، الطبعة الأولى، 2019، ص98.

[2] David L. Anderson، Robert T. Arrigo، Andy Schmidgall; Artificial Intelligence: Can a Machine Think? National Science Foundation Grants، 2006، p.1. On this website;http://www.mind.ilstu.edu/curriculum/ai_can_a_machine_think/ai_machine_think_1.php?modGUI=228&compGUI=1785&itemGUI=3093

[3] رغم ما أوصى به الاتحاد الأوروبي من خلال استراتيجيته للتعامل مع الذكاء الاصطناعي" Une approche européenne de l’intelligence artificielle "، على الموقع التالي بتاريخ دخول 2022/8/10، الساعة1:10م:

المجرد لتطبيقات الذكاء الاصطناعي أياً كان مسمّاها وحتى ولو كانت مهمتها الأساسية هي التحريف والتلفيق والكذب، وربما يرجع ذلك الأمر إلى أن القاعدة العامة هو تجريم السلوك لا الوسيلة، باعتبار أن السلوك مآله انتهاك مصلحة جوهرية، أما الوسيلة لا عقاب على مجرد استخدامها إلا إذا كانت عنصراً من عناصر جريمة معينة وهي تلك التي تسمى بالجرائم محددة الوسيلة[1]، فالمشرع لا يجعل للوسيلة اعتبار إلا إذا كان لها دور بارز في الفعل المكون للركن المادي للجريمة ليكون من خلالها أكثر جسامة وأشد وطأة، وما يعزي هذا الاتجاه أن تطبيقات التزييف العميق قد لا تستخدم لغرض إجرامي وإنما لصناعة محتوى الأفلام والإعلانات والترفيه والمؤثرات البصرية، إضافة إلى خدمة العملاء (المساعد الافتراضي) وإذاعة الأخبار (مقدم الأخبار الافتراضي). بناء عليه لا عقاب على من يستخدم تطبيقات التزييف العميق في تلك الأغراض المشروعة، ولا عقاب على من يستخدم

---

https://digital-strategy.ec.europa.eu/fr/policies/european-approach-artificial-intelligence

[1] ومن أمثلة الجرائم محددة الوسيلة التي يستلزم فيها المشرع وسيلة معينة ما نصت عليه المادة 336 والتي مفادها أنه "يعاقب بالحبس كل من توصل إلى الاستيلاء على نقود أو عروض أو سندات دين أو سندات مخالصة أو أي متاع منقول وكان ذلك بالاحتيال لسلب كل ثروة الغير أو بعضها إما باستعمال طرق احتيالية من شأنها إيهام الناس بوجود مشروع كاذب أو واقعة مزورة أو إحداث الأمل بحصول ربح وهمي أو تسديد المبلغ الذي أخذ بطريق الاحتيال أو إيهامهم بوجود سند دين غير صحيح أو سند مخالصة مزور وإما بالتصرف في مال ثابت أو منقول ليس ملكاً له ولا له حق التصرف فيه وإما باتخاذ اسم كاذب أو صفة غير صحيحة، أما من شرع في النصب ولم يتممه فيعاقب بالحبس مدة لا تتجاوز سنة.

ويجوز جعل الجاني في حالة العود تحت ملاحظة البوليس مدة سنة على الأقل وسنتين على الأكثر.

ذات التطبيقات بغرض التعلم والتدريب أياً كان محتوى ما يقوم به من تجارب طالما لم يمس المصالح الجوهرية المحمية جنائياً، لأن القصد الجنائي انتفى في الحالتين. ولكن إذا ما شرع الجاني بتوليد مقاطع جنسية غير حقيقية باستخدام بيانات شخص معين من خلال ذات التطبيقات **فهل يدخل فعله في إطار العمل التحضيري طالما لم يتم نشره فلا يعاقب عليه أم أنه فعل مجرم استقلالاً؟**

مرحلة التحريف أو التلفيق عبّر عن مدلولها المشرع المصري بـ"المعالجة الإلكترونية" في القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات ووفقاً للمادة الأولى من الباب الأول المعالجة الإلكترونية هي أي عملية إلكترونية أو تقنية تتم كليًا أو جزئيًا لكتابة أو تجميع، أو تسجيل، أو حفظ، أو تخزين، أو دمج، أو عرض، أو إرسال، أو استقبال، أو تداول، أو نشر، أو محو، أو تغيير، أو تعديل، أو استرجاع، أو استنباط للبيانات والمعلومات الإلكترونية، وذلك باستخدام أي وسيط من الوسائط أو الحاسبات أو الأجهزة الأخرى الإلكترونية أو المغناطيسية أو الضوئية أو ما يُستحدث من تقنيات أو وسائط أخرى. وبالتالي قد تتم هذه المعالجة من خلال برنامج معلوماتي[1] أو تقنية معلوماتية[2] كبرامج

---

[1] وفقا للمادة الأولى من قانون 175 لسنة 2018 المصري، البرنامج المعلوماتي: مجموعة الأوامر والتعليمات المعبر عنها بأية لغة أو رمز أو إشارة، والتي تتخذ أي شكل من الأشكال، ويمكن استخدامها بطريق مباشر أو غير مباشر في حاسب آلي لأداء وظيفة أو تحقيق نتيجة سواء كانت هذه الأوامر والتعليمات في شكلها الأصلي أو في أي شكل آخر تظهر فيه من خلال حاسب آلي، أو نظام معلوماتي.

[2] وفقاً للمادة الأولى من قانون 175 لسنة 2018 المصري، تقنية المعلومات: أي وسيلة أو مجموعة وسائل مترابطة أو غير مترابطة تُستخدم لتخزين، واسترجاع، وترتيب، وتنظيم،

وتطبيقات التزييف العميق، رغم أن المشرع لم يذكر ذلك صراحة إلا أنه لا مضار من فهم النص على هذا النحو لأن المشرع عدد أغراض العمليات الإلكترونية على سبيل المثال لا الحصر فيجوز أن يقاس عليها ويضاف لها غيرها، وإن كان من الأفضل أن يضيف المشرع كلمة "تزييف" ضِمن أغراض العمليات الإلكترونية التي عدّدها في نص المادة الآنف ذكره، لأن التزييف هو تخليق وقائع غير حقيقية، فهو مصطلح أدق وأشمل من مجرد الاستنباط أو الدمج أو التعديل أو تغيير البيانات التي أوردها على سبيل المثال في نص المادة.

وتنص المادة 26 من القانون ذاته بأن "يعاقب ... كل من تعمد استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية للغير لربطها بمحتوى منافٍ للآداب العامة، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه".

هناك عدة ملاحظات على نص المادة نوردها في الآتي:

أولاً: أنزل المشرع المصري عقابه على من يضطلع بمعالجة **معطيات شخصية**، ورغم أن المشرع همّ بتعريف مصطلحات هذا القانون في مادته الأولى (الأحكام العامة–التعريفات)، إلا أنه لم يذكر تعريف "المعطيات الشخصية"، واقتصر على تعريف البيانات والمعلومات الإلكترونية[1]،

ومعالجة، وتطوير، وتبادل المعلومات أو البيانات، ويشمل ذلك كل ما يرتبط بالوسيلة أو الوسائل المستخدمة سلكيًا أو لاسلكيًا.

[1] البيانات والمعلومات الإلكترونية: كل ما يمكن إنشاؤه أو تخزينه، أو معالجته، أو تخليقه، أو نقله، أو مشاركته، أو نسخه بواسطة تقنية المعلومات؛ كالأرقام والأكواد والشفرات والحروف والرموز والإشارات والصور والأصوات، وما في حكمها.

والبيانات الشخصية[1]. كما أن المشرع المصري لم يعرّف "المعطيات الشخصية" في القانون رقم ١٥١ لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية رغم حداثته. ونرى أن لا فارق بين مصطلح "معطيات شخصية" و"بيانات شخصية" وإن كان من حُسن صياغة النص القانوني وبخاصة النص الجنائي أن يُوحد المشرع المصطلحات في متون المواد حتى لا يتوهم القارئ وجود اختلاف بين المصطلحين، وإلا ما سبب وجود مادة كاملة للتعريفات في مستهل القانون؟ مع الأخذ في الاعتبار أن العرف جرى بإحالة التعريفات على الفقه القانوني لا النص التشريعي، إلا أنه لا مؤاخذة من أن يبادر المشرع بهذه المهمة بغرض التسهيل على غير المتخصصين، لذا حريّ على المشرع أن يستبدل مصطلح "معطيات شخصية" بـ "بيانات شخصية" اتساقاً مع التعريفات التي ذكرها من ناحية ولتوحيد صياغة النص من ناحية أخرى كما استخدمها في المادة 25 من القانون ذاته بقوله "..... أو منح **بيانات شخصية** إلى نظام أو موقع إلكتروني لترويج السلع أو الخدمات دون موافقته...".

ولما كانت المعطيات الشخصية والبيانات الشخصية سيان من حيث التعريف وهي أي بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده، بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى[2].

---

[1] والبيانات الشخصية: أي بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده، بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى.

[2] جدير بالذكر أن المشرع المصري عرف البيانات الشخصية مرتين، الأولى وفقاً للقانون رقم 175 لسنة 2018 بأنها: بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده، بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى. والأخرى وفقا للقانون رقم 151 لسنة 2020 بأنها: أي بيانات متعلقة بشخص طبيعي محدد، أو يمكن

فإن الصور الثابتة والمتحركة والتسجيلات الصوتية ومقاطع الفيديو أياً كانت مدتها المستخدمة لتغذية تطبيقات التزييف العميق تدخل بما لا يدع مجالاً للشك ضمن البيانات الشخصية المحمية جنائياً، من ثم فعملية المعالجة إذا ما اقترنت بمجموعة من الشروط الأخرى التي نُصَّ عليها في المادة أصبح معاقباً عليها باعتبارها جريمة تامة لا عملاً تحضيرياً.

ثانيا: اشترط المشرع للعقاب على تحريف وتزييف البيانات الشخصية أن يكون المجني عليه **من الغير**، وبالتالي من يضطلع بمعالجة بياناته الشخصية لنفسه لا يندرج تحت مظلة نص المادة حتى ولو كان المحتوى مناف للآداب العامة، وحتى لو كان من شأن المحتوى المساس بشرفه وسمعته واعتباره، طالما لم يضطلع بنشره على الإنترنت أو الإعلان عنه بأي صورة إلكترونية كانت سواء بإرساله للعامة من خلال البريد الإلكتروني أو

تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخرى كالاسم، أو الصوت، أو الصورة، أو رقم تعريفي، أو محدد للهوية عبر الإنترنت، أو أي بيانات تحدد الهوية النفسية، أو الصحية، أو الاقتصادية، أو الثقافية، أو الاجتماعية. ولا نجد فارقاً بين التعريفين سوى أن المشرع عدد بعض البيانات في القانون الأخير غير إنها ذكرت على سبيل المثال لا الحصر. الأمر الذي يدعو للتساؤل حول جدوى تكرار التعريفات، ما من شأنه تضخم المتون الجنائية بلا داعي، لذا كان حري على المشرع ان يكتف بأحدهما عن الآخر. غير أن القانون الجديد لحماية البيانات الشخصية رقم 151 لسنة 2020 كان أكثر تفصيلاً بتناوله لتعريف البيانات الشخصية الحساسة وهي البيانات التي تفصح عن الصحة النفسية أو العقلية أو البدنية أو الجينية، أو بيانات القياسات الحيوية "البيومترية" أو البيانات المالية أو المعتقدات الدينية أو الآراء السياسية أو الحالة الأمنية، وفي جميع الأحوال تعد بيانات الأطفال من البيانات الشخصية الحساسة.

بإرفاقه على مواقع الكترونية أو غيرها من وسائل[1]، من ثم لا عقاب على من يقُم بتوليد وإنتاج مقطع فيديو مزيف لنفسه دون أن يضطلع بنشره، باستثناء الحالة التي يدمج فيها صوراً وتسجيلات صوتية لشخص آخر فيسأل جنائياً في هذه الحالة عن هذا الفعل، كمن يصطنع مقطع فيديو جنسي مزيف لنفسه مع إحدى الفنانات.

كما يقصد بالغير أي شخص ذكراً أو أنثى، أو غيرهما كالمُشكل[2]، سواء كان من الشخصيات العامة أو الفنانين أو من الأفراد العاديين، سواء كان على علاقة سابقة بالجاني أو لا، طالما كانت بياناته الشخصية كفيلة بتحديده وتعيينه، سواء كان طفلاً أو كهلاً، كما يستوى أن يكون محل البيانات المستخدمة لإنتاج الفيديو المزيف شخص من الشرفاء أو من غيرهم، وبالتالي إذا ما استخدم الجاني بيانات شخصية لامرأة عاهرة أو تشتهر بسوء سمعتها لإنتاج فيديو مزيف بواقعة جنسية لم تقترفها يكون آثماً جنائياً ولا يمكن الدفع وقتئذ بسوء سلوك الضحية المُسبق، وهو ما يعطي انطباعاً

---

[1] وفي هذه الحالة تتطابق الأفعال مع ما نص عليه المادتان 1 و14 من قانون مكافحة الدعارة رقم 10 لسنة 1961، فالأولي تنص على «كل من حرض شخصًا ذكرًا كان أو أنثى على ارتكاب الفجور أو الدعارة أو ساعده على ذلك أو سهله له، وكذلك كل من استخدمه أو استدرجه أو أغواه بقصد ارتكاب الفجور أو الدعارة يعاقب بالحبس مدة لا تقل عن سنة ولا تزيد على ثلاث سنوات وبغرامة من مائة جنيه إلى ثلاثمائة جنيه». وتنص المادة 14 من ذات القانون على أن «كل من أعلن بأي طريقة من طرق الإعلان دعوة تتضمن إغراء بالفجور أو الدعارة أو لفت الأنظار إلى ذلك، يعاقب بالحبس مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على مائة جنيه»،

[2] وذلك لأن كلمة الغير الواردة في نص المادة جاءت مطلقة، بالتالي تشمل كل إنسان حيّ أيا كان جنسه حتى ولو كان مشكل أي الشخص الذي أشكل حاله، ولم يتبين هل هو من الرجال؟ أم من النساء؟

بتجريم مجرد الكذب أو تلفيق أو فبركة الوقائع المنافية للآداب في مقاطع فيديو باستخدام أدوات الذكاء الاصطناعي.

أخيراً يخرج الموتى عن مفهوم "الغير"، فمن يضطلع باستخدام صور وتسجيلات وفيديوهات الموتى لإنتاج مقطع فيديو مزيف لا يستساغ عقلاً إنه اعتدى على حرمة الحياة الخاصة لهم والتي تتطلب أن يكونوا أحياء، كما أن التزييف الإباحي العميق غرضه الانتقام، فكيف ينتقم صانع المحتوى المزيف من ميت، وكيف للميت أن يشعر بأذى الانتقام؟ وما يعزي هذا الرأي أن كلمة "الغير" ذكرت في قانون العقوبات المصري 21 مرة جميعها دلّت على أن "الغير" إنسان حي[1]، كما أن المشرع المصري لم يُعاقب سوى على من

---

[1] ومثال على ذلك ما نصت عليه المادة 375 مكرر بأنه ".. يعاقب بالحبس مدة لا تقل عن سنة كل من قام بنفسه أو بواسطة **الغير** باستعراض القوة أو التلويح بالعنف أو التهديد.." فيستحيل أن يكون الغير في مفهوم هذه المادة من الأموات، كذلك المادة 375 التي نصت على أنه "يعاقب بالحبس مدة لا تجاوز سنتين وبغرامة لا تزيد على مائة جنيه كل من استعمل القوة أو العنف أو الإرهاب أو التهديد أو تدابير غير مشروعة في الاعتداء أو الشروع في الاعتداء على حق من الحقوق الآتية:

(أولا) حق **الغير** في العمل.

(ثانيا) حق **الغير** في أن يستخدم أو يمتنع عن استخدام أي شخص.

(ثالثا) حق **الغير** في أن يشترك في جمعية من الجمعيات..... " وبالتالي درج المشرع الجنائي على وصف الغير باعتباره إنساناً حياً، وما ينطبق على المادتين السابقتين يمتد للمواد ال 19 الأخرى، لاسيما المواد (30، 76، 86 مكرر، 88 مكرر(ب)، 98 (ب) مكرر، 102 مكرر، 102 (أ) (د)، 116 مكرر، إلخ.... مؤدى تنازع النصوص في معناه الدقيق أن واقعة إجرامية واحدة تخضع لأكثر من نص من نصوص القانون الجنائي، وإزاء هذه الحالة من تنازع النصوص لا مفر من الأخذ بالحلول المعمول بها في هذا الشأن، والتي تتمثل في ترجيح الوصف الخاص بدلا من الوصف العام؛ أو الوصف الجديد على الوصف القديم؛ أو الوصف الأصلي الجديد على الوصف القديم؛ أو الوصف

يتعرض مادياً فقط لجثث الموتى أو المساس بها وفقاً للقواعد العامة[1]، غير أن الجاني قد يُسأل عن هذا الفعل تحت أوصاف جنائية أخرى وبخاصة في حالة نشر تلك المقاطع على الإنترنت كجريمة التحريض على الفسق والفجور.

ثالثاً: لم يجرم المشرع المصري فعل المعالجة استقلالاً لأي بيانات شخصية للغير إلا إذا تم ربطها بمحتوى منافٍ للآداب العامة[2]، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه. وبالتالي أحدهما يكفي لقيام الركن المادي المكون للجريمة ولا يشترط اجتماعهما، ولكن طالما نتحدث عن مرحلة التحريف والتزييف بواسطة تطبيقات الذكاء الاصطناعي وهي مرحلة

الأصلي على الوصف الاحتياطي. وهو ما يتحقق بتطبيق القانون رقم 175 لسنة 2018 باعتبار القانون الخاص والأحدث.

[1] أما المشرع المصري فقد نظمها في المادة 160 من قانون العقوبات رقم 85 لسنة 1937 (المعدل طبعا)، والتي جاء فيها:" يعاقب بالحبس وبغرامة لا تقل عن مائة جنيه ولا تزيد عن خمسمائة جنيه أو بإحدى هاتين العقوبتين من انتهك حرمة القبور أو الجبانات أو دنسها".

[2] يقصد بالآداب العامة مجموعة الأسس والقيم الأخلاقية التي يقوم عليها البنيان الأساسي للمجتمع والتي تؤدي مخالفتها إلى تفكك المجتمع وانحلاله، وفكرة الآداب العامة هي الجانب الأخلاقي لفكرة النظام العام وهي جزء من النظام العام بمعناه الواسع، وهي من القواعد الضرورية للمحافظة على المجتمع من الانحلال ويجب الالتزام بها من الجميع وعدم المساس بها. د. محمود نجيب حسني، الحق في صيانة العرض في الشريعة الإسلامية وفي قانون العقوبات المصري، بدون ذكر دار نشر، 1984، ص5. د. محمد زكي أبو عامر، الحماية الجنائية للعرض، دار النهضة العربية، القاهرة، ١٩٨٦، ص 25. د. سعيد عبد اللطيف حسن، الحماية الجنائية للعرض، دار النهضة العربية، القاهرة، 2004، ص34. د. أشرف توفيق شمس الدين، الحماية الجنائية للحق في صيانة العرض، دار النهضة العربية، القاهرة، 2004، ص13.

سابقة على النشر أو الإظهار كما عبر عنه نص المادة، فيتعين أن يكون المحتوى تم ربطه على نحو مناف للآداب ولا شك أن اصطناع مقطع جنسي مزيف لشخص ما يدخل ضمن هذا النوع من الأعمال، وتقع الجريمة تامة حتى ولو لم يقم الجاني بنشر المقطع الجنسي المفبرك، كما لو أرسله فقط للمجني عليه في رسالة خاصة تمهيدا للانتقام منه بنشره في مرحلة لاحقة. أما الشطر الأخير في نص المادة وهو"..... أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه" فهذه الحالة مرتبطة بمرحلة النشر أو التوزيع أو النقل لا مرحلة المعالجة الآلية للبيانات الشخصية.

بناء عليه فإن معالجة البيانات الشخصية لشخص ما من خلال تزييف صوره وتسجيلاته الصوتية ومقاطع الفيديو المسجلة له لإنتاج فيديو جنسي مفبرك هو جريمة مستقلة وفقاً للتحليل السابق حتى ولو لم يتم نشر هذا المقطع، فعملية التزييف العميق هي عملية مجرمة طالما كان الغرض منها ربط مقطع الفيديو بما هو منافي للآداب العامة. ولا يقدح في تجريم عملية التزييف العميق على هذا النحو أن المشرع لم ينص صراحة على غرض الانتقام الإباحي، إذ لا مراء أن الإباحية أحد صور تلك الأعمال المنافية للآداب، أما الانتقام هو الدافع الباعث على الجريمة وإن كان من الأفضل أن ينص المشرع عليه ويخصص له عقوبة أشد. كما لا يقدح في تجريم علمية التزييف الإباحي العميق التذرع بصعوبة تحديد المسؤول جنائياً وإسناد الجريمة إليه وملاحقته قضائياً، إذ هي مسألة إجرائية أخرى لا دخل لها بالنموذج القانوني للجريمة، وسوف نتناول إشكالياتها في الشطر الثاني من هذه الدراسة.

جدير بالذكر أن المشرع المصري لم يكتفِ بالعقاب على فعل المعالجة الآلية للبيانات الشخصية للغير حال ربطها بما هو مناف للآداب،

بما يحقق بالتبعية تجريم عملية التزييف الإباحي العميق، وإنما عاقب أيضاً على الشروع فيها[1]، **ولكن هل يُتصور تحققّ الشروع في جريمة التزييف الإباحي العميق، وهل يتعارض العقاب على الشروع فيها مع مبدأ مادية الجريمة؟**

لمّا كان الشروع هو جريمة ناقصة تخلفت فيها النتيجة الإجرامية لسبب لا دخل لإرادة الفاعل فيه رغم ارتكاب السلوك كله أو بعضه[2]، فإن الشروع متصور في جرائم الانتقام الإباحي العميق في الحالة التي يشرع فيها الجاني ببدء عملية المعالجة من خلال تسخير الصور الثابتة والمتحركة والتسجيلات الصوتية ومقاطع الفيديو لخوارزميات الذكاء الاصطناعي لتوليد المقطع الجنسي المفبرك، حيث يتم إنشاء هذا المقطع من خلال مُدخلين من مداخل الذكاء الاصطناعي يعتمد المدخل الأول على إنشاء فيديو جديد مستحدث غير حقيقي، بينما يعتمد المدخل الثاني على إدخال التعديلات على هذا الفيديو لجعله أكثر صدقاً[3]. فإذا لم تتحقق النتيجة كلية وهو عدم

---

[1] وهو ما نصت عليه المادة (٤٠) من قانون 175 لسنة 2018 بان "يعاقب كل من شرع فى ارتكاب الجرائم المنصوص عليها بالقانون، يعاقب بما لا يجاوز نصف الحد الأقصى للعقوبة المقررة للجريمة".

[2] د. سمير الشناوي، الشروع في الجريمة، دار النهضة العربية للنشر والتوزيع، القاهرة، ١٩٧١؛ د. حسني الجندي، نظرية الجريمة المستحيلة في القانون المصري المقارن والشريعة الإسلامية، رسالة دكتوراه، جامعة القاهرة، ١٩٨٠؛ د. وديع فرج، الأعمال التحضيرية والبدء في التنفيذ، مجلة القانون والاقتصاد، كلية الحقوق، جامعة القاهرة، س 4، ص 364.

[3] د. احمد محمد فتحي الخولي: المسئولية المدنية الناتجة عن الاستخدام غير المشروع لتطبيقات الذكاء الاصطناعي "الديب فيك نموذجاً"، مجلة البحوث الفقهية والقانونية، جامعة الازهر بدمنهور، العدد السادس والثلاثون، أكتوبر 2021-1443، ص252

توليد المقطع الجنسي المزيف نتيجة لخطأ تقني ما، أو عدم اتباع الخطوات المتوالية بتجاوز أحد الخطوات سهواً في توليد المقطع المفبرك نكون أمام صورة الشروع الناقص[1]، أما لو تم إنتاج المقطع الإباحي المزيف ولكن كانت جودته سيئة لدرجة يُفقد معها ملامح الأشخاص داخله أو كان المقطع مشوهاً في الصوت والصورة لا يتحدد من خلاله الشخصيات المضمّنة داخله فنكون أمام صورة الشروع التام[2].

وحسنا ما فعل المشرع المصري في العقاب على الشروع في هذه الحالة إذ أن حكمة تجريم الشروع والعقاب عليه رغم عدم وقوع النتيجة المحظورة قانوناً تتمثل في أنه ينطوي على "خطر" تحقيق هذه النتيجة. ولئن كان المشرع يهتم في المقام الأول بالضرر الناشئ فعلاً عن الجريمة متجسدة في النتيجة التي وقعت، فهو أيضاً وبنفس الدرجة لا يغفل عن صور في

---

[1] الشروع الناقص يتمثل في وقوع قدر من السلوك المكون للركن المادي للجريمة فالجاني يبدأ إذن في تنفيذ السلوك دون أن يتمه، ويقال أيضاً للشروع الناقص الجريمة الموقوفة. د. السعيد مصطفى السعيد، الأحكام العامة فى قانون العقوبات، مؤسسة المعارف للطباعة والنشر، القاهرة، 1957، ص ٢٢٨ وما بعدها؛ د. محمود محمود مصطفى، شرح قانون العقوبات، دار النهضة العربية، القاهرة، 1987، ص ٢٩٧ وما بعدها.

[2] الشروع التام يبدأ الجاني بتنفيذ السلوك ويتمه فيقع كاملاً دون أن تتحقق النتيجة رغم هذا لأسباب لا دخل لإرادة الفاعل بها ويسمى هذا الشروع التام بالجريمة الخائبة. د. محمود نجيب حسني، الحق في صيانة العرض في الشريعة الإسلامية وفي قانون العقوبات المصري، المرجع السابق، فقرة ٣٥٩، ص ٣٣٣ وما بعدها؛ د. عوض محمد عوض، قانون العقوبات، القسم العام، مؤسسة الثقافة الجامعية، الإسكندرية، 2007م، فقرة ٢٣١، ص ٢٩٣ وما بعدها.

السلوك تنطوي في ذاتها وبالنظر لنية فاعلها على خطر تحقيق هذا الضرر[1].

جدير بالذكر أن إنتاج مقطع فيديو جنسي مشوه على النحو السابق بيانه من خلال تقنية التزييف العميق لا يمكن اعتباره من قبيل التزييف الضحل "Shallowfake"، والتزييف الضحل أو السطحي أو البسيط عكس التزييف العميق مفاده معالجة محتوى الوسائط دون استخدام تكنولوجيا التعلم الآلي والأنظمة الحسابية أو خوارزميات الذكاء الاصطناعي ولكن بطريقة يدوية[2]، ورغم اختلاف الآلية في نوعي التزييف إلا أنهما يظلان فعلان

---

[1] د. سليمان عبد المنعم: النظرية العامة لقانون العقوبات، المرجع السابق، ص433.

[2] يختلف التزييف العميق عن التزييف الضحل في الآتي؛ أولاً: طريقة الإنتاج: فالتزييف الضحل برنامج تحرير عام وتكييف يدوي لمحتوى الوسائط الموجود مسبقًا، أما التزييف العميق يعتمد على تغييرات خوارزمية على محتوى الوسائط الموجود مسبقًا عن طريق تغذية البيانات إلى برنامج كمبيوتر. لذا فالأول يعتمد أساسًا على العمل البشري اليدوي بخلاف الثاني.

ثانياً: اعتماد التعلم الآلي: يشير المصطلح "الضحل" ذاته إلى غياب التعلم الآلي العميق في إنتاج مقاطع الفيديو، على خلاف التزييف العميق الذي يعتمد على التعلم الآلي لإنتاج الفيديو المزيف.

ثالثاً: اعتماد الذكاء الاصطناعي: التزييف الضحل يتطلب قدراً هائلاً من المهارة والجهد، بالإضافة إلى جزء من البرنامج الذي يمكّن الشخص من إنشاء محتوى الوسائط المزيف، غير ان الذكاء الاصطناعي لا يعد أحد مراحله ولا يدخل في إنتاج الفيديو الضحل، على خلاف التزييف العميق الذي يعتمد على الذكاء الاصطناعي المكون من مجموعة خوارزميات التعلم العميق اللازمة لتطوير محتوى الفيديو المزيف.

Arnold; What Is the Difference Between a Deepfake and Shallow fake? APRIL 21, 2020, Available at;

مجرمان إذا توافرت فيهم الشروط التي يطلبها القانون باعتبارهما وسائل تحقق النتيجة الإجرامية في الأخير وهي التحريف والتلفيق والكذب لإنتاج فيديو جنسي بغرض الانتقام الإباحي.

وإذا كان الشروع معاقباً عليه في جريمة التزييف الإباحي العميق إلا أن ذلك مرتبط بحدود البدء في تنفيذ الجريمة، وهو ما يرسخه مبدأ مادية الجريمة، إذ لا جريمة بدون سلوك ذو وجود واقعي يفترض قدراً ولو يسيراً من الركن المادي ولو كان جزئياً وهو ما يتحقق به الشروع[1]، أما شراء أو الاشتراك في خوارزميات التزييف العميق، أو حيازة أحد تطبيقاته على هاتفه أو جهازه الحوسبي، أو مجرد تجميع وحيازة صور للفنانين، أو التدريب على كيفية تشغيل برامج التزييف العميق أو غيرها من الأفعال التي لا تعد مظهراً من مظاهر البدء في ارتكاب جريمة التزييف الإباحي العميق تقع جميعها في إطار الأعمال التحضيرية التي لا عقاب عليها[2]، وهذا ما يؤكد أن الشروع في جريمة التزييف الإباحي العميق لا يتعارض مع مبدأ مادية الجريمة.

يتبدى مما سبق أن التزييف الإباحي بواسطة تطبيقات التزييف العميق معاقباً عليها كجريمة تامة في حالة إنتاج وتوليد مقطع الفيديو الجنسي المفبرك، كذلك الشروع في الجريمة معاقباً عليه بما لا يجاوز نصف الحد الأقصى للعقوبة المقررة للجريمة في الحالة التي لم يستطع فيها الجاني

---

https://deepfakenow.com/what-is-the-difference-between-a-deepfake-and-shallowfake/

(1) د. سليمان عبد المنعم: تراجع مبدأ مادية الجريمة، دار المطبوعات الجامعية، الإسكندرية، 2015، ص35.

(2) V. J. Pinatel, "L'élément matériel de l'infraction devant la criminologie et les sciences de l'homme ", R. S. C. 1967, p. 913.

إنتاج الفيديو الجنسي المزيف أو إذا أنتجه ولكن بشكل معيب بما لا يتضح معه مضمونه أو فحواه.

جدير بالذكر ان دافع الانتقام لدى الجاني يدفعه ليس فقط لإنتاج الفيديو الإباحي المزيف وإنما لإيذاء الضحية، ويتحقق هذا الإيذاء من خلال إرسال هذا المقطع إلى الضحية أو بإرفاقه على المواقع الإباحية أو بتداوله على مواقع التواصل الاجتماعي أو بتوزيعه على الأشخاص من خلال الهاتف المحمول، وكل الأوجه السابقة معاقباً عليها في قانون العقوبات المصري[1]، من خلال المادة ٢٦ من القانون رقم 175 لسنة 2018م لا

---

[1] نصت المادة 178 منه على أن يعاقب.... كل من نشر أو صنع أو حاز بقصد الاتجار أو التوزيع أو الإيجار أو اللصق أو العرض مطبوعات أو مخطوطات أو رسومات أو إعلانات أو صوراً محفورة أو منقوشة أو رسوماً يدوية أو فوتوغرافية أو إشارات رمزية أو غير ذلك من الأشياء أو الصور عامة إذا كانت خادشه للحياء العام".

يمكن اسقاط نص المادة السابقة على جريمة التزييف الإباحي العميق، وبخاصة انه لم يحدد الوسيلة المستخدمة من ثم تصلح أي وسيلة لتكوين هذه الجريمة والتي من بينها تقنية التزييف العميق، كما انه نص على كل من نشر وصنع وحاز... أشياء خادشه للحياء العام، ولا شك أن مقاطع الفيديو الجنسية التي تظهر مواطن العفة لدى المجني عليه من الأشياء وهي بطبيعتها خادشه للحياء سواء كان القصد الجنائي لناشرها غرضه الانتقام أم لا. غير أن العقوبة المقدرة في المادة السابقة لا تتناسب مع خطورة وجسامة هذا السلوك.

نصت كذلك المادة 309 مكرراً من قانون العقوبات المصري على أنه: "يعاقب... كل من اعتدى على حرمة الحياة الخاصة للمواطن، وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانونا، أو بغير رضاء المجني عليه:

أ- استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أيا كان نوعه محادثات جرت في مكان خاص أو عن طريق التليفون.

ب- التقط أو نقل بجهاز من الأجهزة أياً كان نوعه صورة شخص في مكان خاص.

سيما نشر البيانات الشخصية إذا كان من شأنها المساس بشرف شخصه واعتباره؛ حيث تنص على أن: "يعاقب ... كل من تعمد استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية للغير لربطها بمحتوى مناف للآداب العامة، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه". والمقصود بالإظهار هنا أي وسيلة من شأنها خروج الفيديو المزيف من حوزته إلى الغير ولم تشترط المادة محدودية العدد أو

فإذا صدرت الأفعال المشار إليها في الفقرتين السابقتين أثناء اجتماع على مسمع أو مرأى من الحاضرين في ذلك الاجتماع، فإن رضاء هؤلاء يكون مفترضاً.

وتشدد العقوبة وفقاً للمادة 309 مكررا (أ) بقولها: إنه "يعاقب بالحبس كل من أذاع أو سهل إذاعة أو استعمل ولو في غير علانية تسجيلاً أو مستنداً متحصلاً عليه بإحدى الطرق المبينة بالمادة السابقة أو كان ذلك بغير رضاء صاحب الشأن.

ويعاقب بالسجن مدة لا تزيد على خمس سنوات كل من هدد بإفشاء أمر من الأمور التي تم التحصل عليها بإحدى الطرق المشار إليها لحمل شخص على القيام بعمل أو الامتناع عنه".

كما عاقب المشرع المصري في المادة 73 من قانون تنظيم الاتصالات الصادر بالقانون رقم 10 لسنة ٢٠٠٣م على إتاحة الأمور الشخصية، وذلك بقولها: إنه " يعاقب... كل من قام أثناء تأدية وظيفته في مجال الاتصالات أو بسببها بأحد الأفعال الآتية:

1- إذاعة أو نشر أو تسجيل لمضمون رسالة اتصالات أو لجزء منها دون أن يكون له سند قانوني في ذلك. ٢-..... ٣-..... 4- إفشاء أية معلومات خاصة بمستخدمي شبكات الاتصال أو عما يجرونه أو ما يتلقونه من اتصالات، وذلك دون وجه حق".

كما عاقب قانون مكافحة جرائم تقنية المعلومات المصري لسنة ٢٠١٨ م في المادة ٢٥ منه على انتهاك الخصوصية بنصه على أن: "يعاقب.... كل من اعتدى على أي من المبادئ أو القيم الأسرية في المجتمع المصرى أو انتهك حرمة الحياة الخاصة، أو.....، أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات أو أخباراً أو صوراً وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة".

اتساع نطاقه بل يتحقق الإظهار إذا تم لشخص واحد كما لو أُرسل لشخص الضحية فقط بواسطة أحد تطبيقات الرسائل الخاصة كالواتس آب.

وحسناً ما فعل المشرع أنه استخدم لفظ "الإظهار" بدلاً عن "النشر"، حيث ان النشر يرتكن على العلانية، وهي تعني اتصال علم الجمهور بمعنى مؤذ معين[1]، وذلك بالتعبير عنه بالقول أو الفعل أو الكتابة أو بأية وسيلة أخرى من وسائل التعبير تدخل من ضمنها وسائل التواصل الاجتماعي[2] أو على المواقع الالكترونية باعتبارها من جرائم النشر[3]، لما يشكله من خطورة

---

[1] وتتوفر العلانية في كافة جرائم النشر المرتكبة عبر شبكة الإنترنت بما فيها وسائل التواصل الاجتماعي وذلك لطبيعتها وخصائصها التي سبق وأن تناولناها، إذ تعتبر وسائل التواصل الاجتماعي مكان عام بطبيعتها، بحيث يمكن التعبير من خلالها لعامة المشتركين ومن يمكنهم الاطلاع على المحتوى بمختلف وسائل التعبير كالكتابة وبث التسجيل الصوتي وكذلك المرئي حياً كان أو مسجلاً وأيضاً بالرموز والصور. د. حوراء موسى: الجرائم المرتكبة عبر وسائل التواصل الاجتماعي: دراسة مقارنة، در النهضة العربية، القاهرة، 2018م، ص131.

[2] ومنها تويتر twitter وفيسبوك Facebook وانستغرام Instagram وسناب شات Snapchat ويوتيوب YouTube.

[3] نصت المادة 171 من قانون العقوبات المصري على طرق العلانية بقولها "....
ويعتبر القول أو الصياح علنياً إذا حصل الجهر به أو ترديده بإحدى الوسائل الميكانيكية في محفل عام أو طريق عام أو أي مكان آخر مطروق أو إذا حصل الجهر به أو ترديده بحيث يستطيع سماعه من كان في مثل ذلك الطريق أو المكان أو إذا أذيع بطريق اللاسلكي أو بأية طريقة أخرى.
ويكون الفعل أو الإيماء علنياً إذا وقع في محفل عام أو طريق عام أو في أي مكان آخر مطروق أو إذا وقع بحيث يستطيع رؤيته من كان في مثل ذلك الطريق أو المكان.

على القيم والمصالح المشمولة بالحماية القانونية[1]. أمّا ما يتم من تراسل في الرسائل الخاصة المتوفرة كخدمة في وسائل التواصل الاجتماعي كتطبيقات "ماسنجر، والواتس آب، وسكايب"، فإنها لا تخضع لأحكام العلانية لطبيعة التراسل الخاص الذي يترتب على إفشاءه جريمة انتهاك الخصوصية في غير الحالات المصرح بها قانوناً، ذلك أنه يشترط في القول بعلانية الجريمة أن ترتكب في مكان عام سواء كان مكان عام بطبيعته أو مكان عام بالتخصيص أو مكان عام بالصدفة[2]، بالتالي فإن ركن العلانية غير متوفر في تطبيقات التراسل الخاص، أما الإظهار له مدلول أوسع في نطاقه من العلانية، فإرسال المقطع الإباحي المزيف للضحية على أحد تطبيقات التراسل الخاص يتوفر به عنصر الإظهار وبالتالي تتحقق به الجريمة، كما يُعد إظهاراً إذا أطلع الجاني الفيديو الإباحي المزيف على الغير دون أن يرسله أو ينقله كما لو أراه

وتعتبر الكتابة والرسوم والصور الشمسية والرموز وغيرها من طرق التمثيل علنية إذا وزعت بغير تمييز على عدد من الناس أو إذا عرضت بحيث يستطيع أن يراها من يكون في الطريق العام أو أي مكان مطروق أو إذا بيعت أو عرضت للبيع في أي مكان".

[1] د. شريف السيد كامل، المسؤولية الجنائية للاشخاص المعنوية، دار النهضة العربية للنشر والتوزيع، القاهرة، 1997م، ص 46.

[2] "المكان العام بطبيعته هو كل مكان يباح الدخول أو المرور فيه لأي شخص وفي أي وقت ولو كان خالياً من الناس، حيث يكون من المحتمل دائما سماعه ولو ثبت أن أحدا لم يسمعه، أما بالنسبة للمكان العام بالتخصيص فهو المكان الذي يباح فيه الدخول لأي شخص ولكن في أوقات معينة ويمتنع عليهم الدخول في غير هذه الأوقات كدور العبادة والمسرح والجامعات، أما بالنسبة لمكان العام بالصدفة فإنه في الأصل مكان خاص لكنه يسمح للجمهور بالدخول فيه بصفة عارضة كالمطاعم والمحلات التجارية، حيث يتم الدخول إلى هذه الأماكن في أوقات غير محددة، وعليه فإنها لا تكتسب صفة المكان العام إلا في حال وجود جمهور من الناس فيه وقت الجهر". د. فوزية عبدالستار، شرح قانون العقوبات القسم الخاص، دار النهضة العربية، القاهرة، 1987م، ص 576 وما يليها.

المقطع من خلال هاتفه أو جهازه الحوسبي، كما يُعد إظهاراً من يضع الفيديو الإباحي المزيف كـ"حالة أو قصة"[1] على أحد حساباته الشخصية في تلك التطبيقات الإلكترونية كـ"فيس بوك وانستجرام"، ومن باب أولى كل فعل من شأنه أن يتصل علم الغير بالفيديو الإباحي المزيف يعد إظهاراً كالنشر على وسائل التواصل الإجتماعي أو إرفاقه على المواقع الإلكترونية الإباحية أو الإرسال على البريد الإلكتروني أو نقله أو توزيعه أو غيرها من الوسائل التي يتحقق بها الإظهار، من ثم يكون مصطلح "الإظهار" أكثر دلالة واستغراقا لكافة وسائل وطرق العلم من مصطلح "النشر".

نخلُص مما سبق أن السلوك المكون للركن المادي لجريمة التزييف الإباحي العميق متتابع الأفعال، يبدأ بجمع البيانات الشخصية، ثم تغذية التطبيقات الخاصة بالتزييف العميق وإنتاج الفيديو الإباحي المفبرك، وأخيرا إظهار هذا الفيديو، واتضح مما سبق ان المشرع المصري عاقب استقلالاً على عملية توليد وإنتاج الفيديو الإباحي المزيف بغرض الانتقام، إلا أن لاكتمال النصاب القانوني للجريمة يتعين أن يكون القصد الجنائي حاضراً من خلال توافر الركن المعنوي لجريمة التزييف الإباحي العميق.

2- الركن المعنوي

---

[1] الحالات أو القصص هي مجموعة من مقاطع الفيديو القصير التي لا تتعد 30 ثانية يتم ارفاقها على التطبيق، غير جميع الحالات التي يتم مشاركتها تختفي تلقائياً بعد 24 ساعة من نشرها. جدير بالذكر أن الحالات والقصص تكون وبشكل افتراضي مرئية لدى جميع الأشخاص الذين يمتلك الجاني أرقامهم ويملكون رقمه، لكن يُمكن أن توجه تلك الحالات لأناس معينين باستثناء بعضهم. ويتم انشاء الحالات من خلال مجموعة بسيطة من الخطوات، المزيد على الرابط التالي بتاريخ دخول 2022/8/11 الساعة 12:50م
https://faq.whatsapp.com/2538892862990242/?locale=ar_AR

جريمة الانتقام الإباحي عبر تقنية التزييف العميق من الجرائم العمدية[1]، ويستمد العمد في هذه الجريمة من صراحة نص المادة 26 بقولها "يعاقب ... كل من **تعمد** استعمال برنامج معلوماتى.....". من ثم فيشترط لقيام هذا الركن ان يكون الجاني عالماً ان ما يقوم به هو تزييف وتلفيق وكذب باستخدام تقنية التزييف العميق لبيانات شخصية لإنسان حي بغرض توليد مقطع فيديو إباحي له كواقعة وهمية لم تحصل فعلياً على أرض الواقع، كما يشترط أن تتجه إرادة الجاني لإحداث هذا النشاط أو السلوك.

لم يتطلب المشرع المصري قصداً خاصاً لهذه الجريمة بل اكتفى بتوافر القصد العام، وبالتالي يستوي ان يكون إنتاج وتوليد الفيديو المزيف بغرض الانتقام أو بغرض الارتزاق أو بغرض التفاخر بالنفس أو إرضاء شعور غريزي لديه أو غيرها من الأغراض، ولئن كان القصد الجنائي أو العمد يقوم بمجرد توافر عنصري العلم والإرادة، فإن مؤدى ذلك عدم اعتبار الباعث أو الدافع عنصراً في هذا القصد[2]. والباعث أو الدافع هو الغاية

---

[1] والجريمة العمدية هي تلك التي يتطلب المشرع لقيامها القصد الجنائي، والقصد الجنائي قوامه الإرادة، والعلم: 1- إرادة السلوك بطبيعة الحال (وهي عنصر مشترك بين الجرائم العمدية وغير العمدية)؛ ٢- إرادة أو "نية" تحقيق النتيجة المحظورة قانونا؛ 3- العلم بكافة العناصر الواقعية الجوهرية اللازمة لقيام الجريمة؛ 4- العلم بصلاحية السلوك لإحداث النتيجة؛ ويلاحظ أن العلم في هذا العنصر الأخير قد يأخذ صورة اليقين فيكون القصد مباشراً، وقد يأخذ صورة الاحتمال فيقال له القصد الاحتمالي أو غير المباشر، وفي الحالتين نكون بصدد جريمة عمدية. د. سليمان عبد المنعم: النظرية العامة لقانون العقوبات، المرجع السابق، ص228.

[2] ورغم ذلك فقد يعتبر الدافع على الجريمة في حالات حد استثنائية عنصراً من عناصرها أو معياراً لإضفاء طبيعة معينة عليها. فقد يجعل المشرع من الدافع عنصراً لا تقوم الجريمة إلا به كما في جريمة استغلال البغاء المنصوص عليها في المادة 65 فقرة ثانية

الشخصية أو الغرض البعيد الذي يتوخاه الجاني من جراء ارتكابه الجريمة وهو الانتقام في الجريمة محل البحث غير ان القصد الجنائي يقوم لدى الجاني بصرف النظر عن الباعث الذي حدا به إلى ارتكاب الجريمة.

رابعاً: العقوبة المقررة

تنص المادة 26 من القانون رقم 175 لسنة 2018م على أن: "يعاقب بالحبس مدة لا تقل عن سنتين ولا تجاوز خمس سنوات وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز ثلاثمائة ألف جنيه أو بإحدى هاتين العقوبتين كل من تعمد ....". من ثم يعاقب على جريمة التزييف الإباحي العميق باعتبارها أحد جرائم معالجة المعطيات الشخصية للغير بعقوبة تخييرية إما الحبس والغرامة معاً أو الحبس أو الغرامة. ولعلّ موقف المشرع هنا يثير التساؤل حول شبهة التناقض، فقد قرر رفع الحدين الأدنى والأقصى لعقوبة الحبس لتتراوح بين سنتين و5 سنوات، بدلاً عن 24 ساعة و3 سنوات وفقاً للقواعد العامة[1]، مما لا يجوز معه وقف تنفيذ هذه العقوبة[2]، وذلك

من القانون رقم 10 لسنة 1961م بشأن مكافحة الدعارة إذ لا تقوم هذه الجريمة إلا إذا كان الكسب هو الدافع إلى ارتكابها. نقض جنائي مصري، بتاريخ جلسة ٢٠ إبريل ١٩٤٢م، مجموعة القواعد القانونية، ج 5، ق ٣٨٨، ص ٦٤٦؛ وكذلك جلسة 4 أكتوبر ١٩٤٨م، ح 7، ق 346، ص ٦١٣. د. سليمان عبد المنعم: النظرية العامة لقانون العقوبات، المرجع السابق، ص398.

[1] حيث تنص المادة 18 عقوبات مصري على أن "عقوبة الحبس هي وضع المحكوم عليه في أحد السجون المركزية أو العمومية المدة المحكوم بها عليه ولا يجوز أن تنقص هذه المدة عن أربع وعشرين ساعة ولا أن تزيد على ثلاث سنين إلا في الأحوال الخصوصية المنصوص عليها قانوناً".

[2] حيث تنص المادة 55 عقوبات مصري على أن "يجوز للمحكمة عند الحكم في جناية أو جنحة بالغرامة أو بالحبس مدة لا تزيد عن سنة أن تأمر في نفس الحكم بإيقاف تنفيذ

لاستشعاره خطورة هذه الجريمة إلا أنه في الوقت ذاته جعل العقوبة تخييرية، فمن الوارد إذاً أن يُحكم على الجاني بغرامة مائة ألف جنيه فقط دون غيرها من عقوبات، وهو ما لا يتناسب مع جسامة الفعل وجسامة النتيجة وبخاصة في جريمة التزييف الإباحي العميق، لذا كان حريّ على المشرع أن يجعل العقوبة وجوبية لا تخييرية.

يلاحظ كذلك أن المشرع المصري لم يشدد العقوبة إذا كان الغرض من الجريمة هو الانتقام الإباحي رغم خطورته، وإذا كان الانتقام الإباحي باعتباره باعث دافع لارتكاب الجريمة ليس عنصراً من عناصر الركن المعنوي للجريمة إلا أنه رغم ذلك يؤخذ بالباعث أو الدافع في الاعتبار فيما يتعلق بتقدير العقوبة المحكوم بها على الجاني. فقد يكون الدافع الشائن سبباً لتشديد العقوبة، والدافع النبيل سبباً لتخفيفها استناداً لما يملكه القاضي من سلطة تقديرية يخوله إيّاها المشرع في هذا الخصوص[1]، وهو ما انتهجه المشرع المصري، غير إنه شدّد العقاب في أحوال أخرى ليس من بينها الانتقام الإباحي نصّت عليها المادة 34 من القانون رقم 175 لسنة 2018م وهي "إذا وقعت ... بغرض الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر، أو الإضرار بالأمن القومي للبلاد أو بمركزها الاقتصادي أو

العقوبة إذا رأت من أخلاق المحكوم عليه أو ماضيه أو سنه أو الظروف التي ارتكب فيها الجريمة ما يبعث على الاعتقاد بأنه لن يعود إلى مخالفة القانون. ويجب أن تبين في الحكم أسباب إيقاف التنفيذ.

ويجوز أن يجعل الإيقاف شاملاً لأية عقوبة تبعية ولجميع الآثار الجنائية المترتبة على الحكم".

[1] فالمادة 17 من قانون العقوبات المصري تجيز في مواد الجنايات تخفيف العقوبة المحكوم بها إذا اقتضت أحوال الجريمة ذلك.

منع أو عرقلة ممارسة السلطات العامة لأعمالها، أو تعطيل أحكام الدستور أو القوانين أو اللوائح أو الإضرار بالوحدة الوطنية والسلام الاجتماعي تكون العقوبة السجن المشدد". لذا كان حريّ على المشرع أن يضيف إلى الأغراض إلى عددها لتشديد العقوبة غرض الانتقام الإباحي.

تمتد العقوبة الجنائية كذلك للأشخاص الاعتبارية بموجب صراحة نص المادة ٣٦ من القانون ذاته في الأحوال التي ترتكب فيها جريمة التزييف الإباحي العميق باعتبارها أحد جرائم معالجة المعطيات الشخصية للغير، باسم ولحساب الشخص الاعتباري، ويعاقب المسئول عن الإدارة الفعلية إذا ثبت علمه بالجريمة أو سهل ارتكابها تحقيقاً لمصلحة له أو لغيره بذات عقوبة الفاعل الأصلي. وللمحكمة أن تقضى بإيقاف ترخيص مزاولة الشخص الاعتباري للنشاط مدة لا تزيد على سنة، ولها فى حاله العود أن تحكم بإلغاء الترخيص أو حلّ الشخص الاعتباري بحسب الأحوال، ويتم نشر الحكم فى جريدتين يوميتين واسعتي الانتشار على نفقة الشخص الاعتباري.

ولا يترتب على تقرير مسئولية الإدارة الفعلية للشخص الاعتبارى استبعاد المسئولية الجنائية للأشخاص الطبيعيين الفاعلين الأصليين أو الشركاء عن ذات الوقائع التى تقوم بها الجريمة وفقاً لما نصّت عليه المادة 37 من القانون ذاته.

أما بخصوص العقوبات التكميلية فقد نصّت المادة 38 على أنه "مع عدم الإخلال بحقوق الغير حسن النية، على المحكمة فى حالة الحكم بالإدانة فى أى جريمة من الجرائم المنصوص عليها فى هذا القانون، أن تقضى بمصادرة الأدوات والآلات والمعدات والأجهزة مما لا يجوز حيازتها قانوناً، أو غيرها مما يكون قد استخدم فى ارتكاب الجريمة، أو سهل أو ساهم فى ارتكابها.

وفى الحالات التى يتعين لمزاولة النشاط فيها الحصول على ترخيص من إحدى الجهات الحكومية، وكان الشخص الاعتبارى المدان بأى جريمة منصوص عليها فى هذا القانون لم يحصل على الترخيص فيحكم فضلاً عن العقوبات المقررة بالغلق"[1].

أما بخصوص الإعفاء من العقاب فقد نصت المادة (٤١) على ان "يعفى من العقوبات، المقررة للجرائم المنصوص عليها في هذا القانون، كل من بادر من الجناة أو الشركاء إلى إبلاغ السلطات القضائية أو السلطات العامة بما يعلمه عنها قبل البدء في تنفيذ الجريمة وقبل كشفها.

ويجوز للمحكمة الإعفاء من العقوبة أو التخفيف منها إذا حصل البلاغ بعد كشف الجريمة وقبل التصرف في التحقيق فيها، إذا مكن الجاني أو الشريك في أثناء التحقيق السلطات المختصة من القبض على مرتكبي الجريمة الآخرين، أو على ضبط الأموال موضوع الجريمة، أو أعان أثناء البحث والتحقيق على كشف الحقيقة فيها، أو على القبض على مرتكبي جريمة أخرى مماثلة لهذا النوع والخطورة". وإذا تقرر الإعفاء سواء كان وجوبياً أو جوازياً فإنه يقتضي رد المال المتحصل من الجريمة وفقا لما نصّت عليه المادة 41 في فقرتها الثالثة من القانون رقم 175 لسنة 2018م.

---

[1] كما نصت المادة ٣٩ أنه "للمحكمة إذا قضت بالإدانة على أحد الموظفين العموميين، لارتكابه جريمة من الجرائم المنصوص عليها فى هذا القانون، أثناء وبسبب تأديته لوظيفته، أن تقضى بعزله مؤقتاً من وظيفته، إلا فى الحالات المشار إليها فى المادة (٣٤) من هذا القانون فيكون العزل وجوبياً".

المبحث الثاني

المسؤولية الجنائية عن جريمة الانتقام الإباحي عبر تقنية التزييف العميق "Deepfakes"

تمهيد

المسؤولية بوجه عام، هي تحمُّل التّبِعة[1]، حيث يعبأ الشخص بنتيجة أفعاله إذا سبّب فعله ضرراً للغير[2]، ولا مراء من مُساءلة مستخدم برامج التزييف العميق جنائياً عن جريمة الانتقام الإباحي العميق، كذلك مُتصيد البيانات الشخصية بالإضافة إلى ناشر المقطع الجنسي المفبرك ومشاركه، سواء كانوا فاعليين أصليين في الجريمة أم مشاركين فيها، إلا أن الإشكالية تدق وبحق في الحالة التي يُصمم فيها برنامج التزييف العميق لغرض سينمائي أو فني، ويضطلع عن طريق الخطأ بإنشاء محتوى جنسي لأحد الفنانين دون تدخل من مستخدم ودون علم مصنع البرنامج أو منفذ الخوارزمية، وبخاصة أن مناط المسؤولية الجنائية في هذه الجريمة هو "**التزييف الإباحي العميق**" أي التلفيق الجنسي الذي يتم من خلال تقنية "Deepfakes" باعتبار أن تلك التقنية هي العنصر الفاعل في معالجة وإنتاج وتوليد المقطع الجنسي المزيف، الأمر الذي يثير معه إشكالية مدى إمكانية مساءلة تلك التقنية جنائياً باعتبارها أحد كيانات الذكاء الاصطناعي، وبخاصة في الفرض الذي تضطلع فيه منفردة بإنتاج وتوليد مقطع جنسي

---

(1) د. محمد كمال الدين إمام: المسؤولية الجنائية أساسها وتطورها: دراسة مقارنة في القانون الوضعي والشريعة الإسلامية، دار الجامعة الجديدة، الإسكندرية، 2004م، ص3.

(2) د. سليمان مرقس: المسؤولية المدنية في تقنينات البلاد العربية، معهد البحوث والدراسات العربية، القاهرة، 1960م، ص380.

مفبرك دون علم المبرمج أو منشئ المحتوى أو جامع البيانات الشخصية، وهذا الفرض لا يخلو من واقعية في ظل التسارع اللحظي لتكنولوجيا الذكاء الاصطناعي المعتمدة على التعلّم الذاتي والتعلّم العميق لتُقارب بل وتتخطى في ذلك ذكاء الإنسان وقدرته على التفكير واتخاذ قرارات مستقلة[1].

إشكالية أخرى ربما تثور حول الملاحقة القضائية لمرتكب هذه الجريمة الذي لا يحتاج لإعدادها وتنفيذها أن يكون داخل إقليم الدولة، فهي جريمة تتسم بالعالمية لإمكانية نشرها على الإنترنت، ونتناول فيما يلي كلاً من مسألة تحديد الأشخاص المسؤولين جنائياً عن الجريمة، وكيفية ملاحقتهم قضائياً على النحو التالي؛

أولاً: تحديد الأشخاص المسؤولين جنائياً

جريمة الانتقام الإباحي عبر تقنية التزييف العميق إنما تتحقق حال اصطناع فيديو جنسي غير حقيقي لشخص ما ثم إظهاره بغرض الانتقام

---

[1] عبير أسعد: الذكاء الاصطناعي، دار البداية، القاهرة، الطبعة الأولى، 2017م، ص3 وما يليها. آلان بونيه: الذكاء الاصطناعي، واقعه ومستقبله، 1945م، ترجمة د. على صبري فرغي، مجلة عالم المعرفة، العدد رقم 172، 1993م، ص69. كذلك؛

Kaplan, Andreas and Haenlein, Michael. (January–February 2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence, Kelley School of Business, Indiana University. Elsevier Inc. Vol.62, I.1, pp.15–25. Rich, Elaine and Knight, Kevin. Artificial Intelligence, McGraw Hill companies Inc. 2006, pp.105–192. Russell, Stuart and Norvig, Peter. Artificial Intelligence: A Modern Approach Prentice Hall, 2002, p.195.

منه، وكما أسلفنا القول إن سلوك هذه الجريمة يمر بعدة مراحل يتعدد معها الأشخاص المسؤولون جنائياً، والتي تبدأ بجمع بيانات الشخص الضحيّة من صور وتسجيلات صوتية ومقاطع فيديو وغيرها، ثم تحريف ومعالجة هذه البيانات لإنتاج الفيديو المزيف بواسطة تطبيقات الذكاء الاصطناعي، وأخيراً إظهار المقطع الجنسي المزيف بأي وسيلة من وسائل الإظهار سواء النشر أو التراسل الخاص أو غيرها من وسائل. لا تثار إشكالية تحديد المسؤول جنائيا عن الجريمة في الحالة التي يرتكب فيها شخص واحد كل الأفعال المتتابعة المكونة للركن المادي لها، وإنما تثور الإشكالية وبحث حال تعددهم ومن منهم يكون فاعلاً أصلياً في الجريمة ومن منهم شريكاً؟

بيد أن أول من يسأل جنائياً إذن هو مُتصيّد البيانات الشخصية، فجمع البيانات الشخصية لا يدخل ضمن العمل المباح بالنسبة لكل من المتحكم[1] والمعالج[2] والحائز[1] للبيانات الشخصية من ثم يكونوا مسؤولون

---

[1] المتحكم: أي شخص طبيعي أو اعتباري يكون له بحكم أو طبيعة عمله، الحق في الحصول على البيانات الشخصية وتحديد طريقة وأسلوب ومعايير الاحتفاظ بها، أو معالجتها والتحكم فيها طبقاً للغرض المحدد أو نشاطه. وفقاً للمادة الأولى من قانون حماية البيانات الشخصية المصري 151 لسنة 2020م.

[2] المعالج: أي شخص طبيعي أو اعتباري مختص بطبيعة عمله، بمعالجة البيانات الشخصية لصالحه أو لصالح المتحكم بالاتفاق معه ووفقاً لتعليماته.

وفى محاولة لتوضيح الفرق بين المقصود بكل من المعالج والمتحكم، نذكر المثالين الآتيين:

المثال الأول: في حالة التعامل مع بيانات العماء في إطار تقديم خدمات الكهرباء، نجد أن مزود الخدمة بمقتضى عقد بينه وبين الشخص المعنى بالبيانات هو شركة الكهرباء والتي تعتبر في هذه الحالة متحكم بالبيانات، بينما نجد أن معالجة البيانات

جنائياً باعتبارهم فاعلين أصليين عمّا يستحوذون عليه من بيانات شخصية بالمخالفة للقانون دون علم أو رضاء صاحبها، حيث نصت المادة 2 من قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020م على أنه "لا يجوز جمع البيانات الشخصية أو معالجتها أو الإفصاح عنها أو إفشائها بأي وسيلة من الوسائل إلا بموافقة صريحة من الشخص المعني بالبيانات، أو في الأحوال المصرح بها قانونًا".[2] واشترط المادة 3 من القانون ذاته في

الاستخراج الفواتير لا يتم من قبل نفس الشركة في مصر وإنما من قبل شركة أخرى، وتعد هذه الأخيرة في تلك الحالة معالجا للبيانات فقط دون أن تكون متحكمة بها.

المثال الثاني: تقديم خدمات النقل الجوي، في هذا الشأن تقدم خدمة النقل الجوي شركة مصر للطيران وهى تحصل على البيانات الشخصية اللازمة لتقديم الخدمة وتتعامل معها بصفتها متحكم، بينما نجد أن عملية معالجة تلك البيانات الاستخراج تذاكر رحلات السفر يتم من قبل شركة أخرى(Amido) والتي تعتبر في هذه الحالة معالجا للبيانات. يرجع في ذلك إلى ورشة عمل تحت عنوان: دراسة نقدية لقانون حماية البيانات الشخصية رقم (151) لسنة 2020م، إعداد مركز بحوث القانون والتكنولوجيا، كلية القانون، الجامعة البريطانية، بالتعاون مع مكتب أندرسن للمحاماة، 12 أكتوبر 2020م، ص39. على الرابط التالي:

https://eg.andersen.com/wp-content/uploads/2021/03/Technical-Analysis-of-Personal-Data-Protection.pdf

[1] والحائز هو: أي شخص طبيعي أو اعتباري، يحوز ويحتفظ قانونيًا أو فعلياً ببيانات شخصية في أي صورة من الصور، أو على أي وسيلة تخزين سواءً أكان هو المنشئ للبيانات، أم انتقلت إليه حيازتها بأي صورة.

[2] وبحسب نص المادة ذاته فإنه "ويكون للشخص المعني بالبيانات الحقوق الآتية:

١ – العلم بالبيانات الشخصية الخاصة به الموجودة لدي أي حائز أو متحكم أو معالج والاطلاع عليها والوصول إليها أو الحصول عليها.

٢ – العدول عن الموافقة المسبقة على الاحتفاظ ببياناته الشخصية أو معالجتها.

٣ – التصحيح أو التعديل أو المحو أو الإضافة أو التحديث للبيانات الشخصية.

فقرتها الأولى بضرورة أن "تُجمع البيانات الشخصية لأغراض مشروعة ومحددة ومعلنة للشخص المعني، بالإضافة لمجموعة ضوابط أخرى"[1].

ويُلاحظ أن المتحكم أو المعالج أو الحائز تجمعهم القدرة على السيطرة على البيانات الشخصية بموجب طبيعة عملهم سواء كانوا أشخاص طبيعيون أم أشخاص اعتبارية كالشركات التجارية وبخاصة شركات التسويق الإلكتروني، وهيئات ومؤسسات الدولة كالسجل المدني، وبنوك المعلومات، وشركات التكنولوجيا المالية، والوسطاء التقنيون، شركات الدفع الإلكتروني وغيرهم. وبالتالي تثور الإشكالية في الحالة التي يتم جمع البيانات فيها من خلال شخص طبيعي لا متحكم ولا معالج ولا حائز بحكم طبيعة عمله؟ فهؤلاء الأشخاص هم المخاطبون بأحكام قانون حماية البيانات الشخصية رقم

---

٤ – تخصيص المعالجة في نطاق محدد.

٥ – العلم والمعرفة بأي خرق أو انتهاك لبياناته الشخصية.

٦ – الاعتراض على معالجة البيانات الشخصية أو نتائجها متي تعارضت مع الحقوق والحريات الأساسية للشخص المعني بالبيانات. وباستثناء البند (٥) من الفقرة السابقة، يؤدي الشخص المعني بالبيانات مقابل تكلفة الخدمة المقدمة إليه من المتحكم أو المعالج فيما يخص ممارسته لحقوقه، ويتولى المركز إصدار قرارات تحديد هذا المقابل بما لا يجاوز عشرين ألف جنيه.

[1] حيث نصت المادة 3 من القانون رقم 151 لسنة 2020 على ان " مادة (٣):

يجب لجمع البيانات الشخصية ومعالجتها والاحتفاظ بها، توافر الشروط الآتية:

١ – أن تجمع البيانات الشخصية لأغراض مشروعة ومحددة ومعلنة للشخص المعني.

٢ – أن تكون صحيحة وسليمة ومؤمنة.

٣ – أن تعالج بطريقة مشروعة وملائمة للأغراض التي تم تجميعها من أجلها.

٤ – ألا يتم الاحتفاظ بها لمدة أطول من المدة اللازمة للوفاء بالغرض المحدد لها.

وتحدد اللائحة التنفيذية لهذا القانون السياسات والإجراءات والضوابط والمعايير القياسية للجمع والمعالجة والحفظ والتأمين لهذه البيانات.

151 لسنة 2020م الأمر الذي يُستثنى معه من المسؤولية الجنائية الأفراد العاديين الذين ليس لهم سيطرة فعلية على البيانات الشخصية، جدير بالذكر ان البيانات التي يحتاجها إنتاج وتوليد فيديو جنسي مزيف من خلال تقنية التزييف العميق ممكن أن تتم من خلال الأفراد العاديين الذين ليس لهم سيطرة فعلية على البيانات بحكم وظائفهم، سواء تمت عملية جمع البيانات بطريقة يدوية من خلال البحث وسحب وحفظ الصور ومقاطع الفيديو والتسجيلات الصوتية المرفقة بالحسابات الشخصية على وسائل التواصل الاجتماعي والمواقع الإلكترونية، أو باستخدام برامج معدّة لذات الغرض مثل"Zoho Creator" أو "webscraper.io" وغيرها من البرامج الإلكترونية المخصصة لسحب وجمع البيانات أو "مستخلِصات البيانات" كما يطلق عليها التقنيون[1].

إضافة إلى ذلك يكون المتحكّم في البيانات والمعالج والحائز مسؤولون جنائياً في حالة اضطلاعهم بجمع البيانات الشخصية دون تصريح[2] أو ترخيص[1] من الجهة المختصة[2]، وهو ما يثير التساؤل أيضاً

---

[1] Nicholas J. DeVito , Georgia C. Richards & Peter Inglesby: How we learnt to stop worrying and love web scraping: Nature, 08 September 2020, Available at: https://www.nature.com/articles/d41586-020-02558-0

[2] التصريح: وثيقة رسمية تصدر عن المركز للشخص الطبيعي أو الاعتباري تمنحه من خلالها الحق في ممارسة نشاط جمع البيانات الشخصية الإلكترونية أو تخزينها أو نقلها أو معالجتها أو القيام بأنشطة التسويق الإلكتروني أو كل ما سبق والتعامل عليها بأي صورة، أو لأداء مهمة أو مهام معينة، وتحدد هذه الوثيقة التزامات المصرح له وفق القواعد

حول المسؤولية الجنائية للأفراد العاديين ممّن ليس لهم سيطرة على البيانات بحكم وظيفتهم إذا ما شرعوا في ممارسة هذا السلوك دون تصريح مسبق؟ جدير بالذكر أنه ليس هناك نص يجرم مجرد جمع البيانات الشخصية المتاحة والمباحة والمرفقة على حسابات الأشخاص على وسائل التواصل الاجتماعي حتى في قانون مكافحة تقنية المعلومات المصري رقم 175 لسنة 2018م[3]، ربما لعدم مخالفة هذا الفعل للحق في الخصوصية

والشروط والإجراءات والمعايير الفنية المحددة باللائحة التنفيذية، لمدة مؤقتة لا تجاوز سنة، ويجوز تجديدها لأكثر من مدة.

[1] الترخيص: وثيقة رسمية تصدر عن المركز للشخص الاعتباري تمنحه من خلالها الحق في مزاولة نشاط جمع البيانات الشخصية الإلكترونية أو تخزينها أو نقلها أو معالجتها أو القيام بأنشطة التسويق الإلكتروني أو كل ما سبق والتعامل عليها بأي صورة، وتحدد التزامات المرخص له وفق القواعد والشروط والإجراءات والمعايير الفنية المحددة باللائحة التنفيذية لهذا القانون، وذلك لمدة ثلاث سنوات قابلة للتجديد لمدد أخرى.

[2] بحسب المادة 19 من قانون حماية البيانات الشخصية المصري رقم 151 لسنة 2020م، تنشأ هيئة عامة اقتصادية تسمي "مركز حماية البيانات الشخصية"، تتبع الوزير المختص، وتكون لها الشخصية الاعتبارية، ويكون مقرها الرئيس محافظة القاهرة أو إحدى المحافظات المجاورة لها، وتهدف إلى حماية البيانات الشخصية وتنظيم معالجتها وإتاحتها، ولها في سبيل تحقيق أهدافها أن تباشر جميع الاختصاصات المنصوص عليها بهذا القانون، ولها على الأخص الآتي: .....

إصدار التراخيص أو التصاريح والموافقات والتدابير المختلفة المتعلقة بحماية البيانات الشخصية وتطبيق أحكام هذا القانون.

اعتماد الجهات والأفراد، ومنحهم التصاريح اللازمة التي تتيح لهم تقديم الاستشارات في إجراءات حماية البيانات الشخصية.

[3] ولا يندرج هذا النمط من تجميع البيانات الشخصية كأحد جرائم الاعتراض غير المشروع للبيانات التي نصت عليها المادة 16 من القانون ذاته بقولها "يُعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتين وخمسين ألف

استناداً على ان أصحاب هذه البيانات تركوها في طرقات الإنترنت دون أدنى حماية تذكر مما يعد تنازلاً ضمنياً عن حقوق سريتها وبالتالي من يضطلع بجمع كافة صور أحد الفنانين لا يُسأل جنائياً عن هذا الفعل بغض الطرف عن استعمال هذه الصور من عدمه وما يسري على الصور يسري على البيانات الأخرى[1]، فضلاً عن ذلك فمجرد جمع البيانات يعد عملا تحضيرياً

جنيه، أو بإحدى هاتين العقوبتين، كل من اعترض بدون وجه حق أى معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلى وما فى حكمها". وبحسب مفهوم الاعتراض الذي نص عليه في المادة الأولى فإنه" الاعتراض: مشاهدة البيانات أو المعلومات أو الحصول عليها، بغرض التنصت أو التعطيل، أو التخزين أو النسخ، أو التسجيل، أو تغيير المحتوى، أو إساءة الاستخدام أو تعديل المسار أو إعادة التوجيه وذلك لأسباب غير مشروعة ودون وجه حق". واستبعاد نموذج جمع البيانات الشخصية كالصور ومقاطع الفيجية والتسجيلات الصوتية وغيرها من جريمة الاعتراض غير المشروع، أن الأخيرة تتشابه مع جريمة التنصت على المكالمات الهاتفية وذلك لأن الاعتراض يهدف للوصول إلى المعلومات المتداولة على منظومة أو شبكة معلوماتية وذلك أثناء تبادلها، فتبادل المعلومات شرط أساسي لقيام جريمة الاعتراض غير المشروع أما المعلومات إذا كانت مخزنة أو ثابتة كالمتاحة على الحسابات الشخصية للأفراد على وسائل التواصل الاجتماعي لا يتحقق به نموذج جريمة الاعتراض، لذا يخرج عن مفهوم الجريمة جمع البيانات المتاحة على وسائل التواصل الاجتماعي. د. طارق الخن: الجرائم المعلوماتية، منشورات الجامعة الافتراضية السورية، 2018م، ص40.

[1] ولا يتعارض ذلك مع تجريم الاعتداء على الحق في الصورة التي نص عليها المشرع المصري في المادة 309 من قانون العقوبات لديه بقولها "يعاقب بالحبس مدة لا تزيد على سنة كل من اعتدى على حرمة الحياة الخاصة للمواطن وذلك بأن ارتكب أحد الأفعال الآتية في غير الأحوال المصرح بها قانوناً أو بغير رضاء المجني عليه:
(أ) استرق السمع أو سجل أو نقل عن طريق جهاز من الأجهزة أياً كان نوعه محادثات جرت في مكان خاص أو عن طريق التليفون.

لا جريمة مستقلة والعقاب عليه يدخل في إطار تجريم النوايا وهو ما يتعارض مع مبدأ مادية الجريمة[1]. وبالتالي يتعين التفرقة بين نوعين من البيانات بحسب معيار الحماية المشمولة بها، أولاً: البيانات الشخصية المحمية، وهي تلك البيانات التي أضفى عليها أصحابها حد أدنى من الحماية بحيث تكون غير منشورة على وسائل التواصل الاجتماعي أو تلك المخزنة على الحوسبات السحابية والتي لا يمكن الولوج إليها إلا باستخدام كلمات مرور خاصة بكل حساب شخصي، أو البيانات الشخصية الموجودة على الهواتف والأجهزة اللوحية الخاصة بالأفراد. ثانياً: البيانات الشخصية المتروكة، وهي تلك البيانات التي تنازل أصحابها عن حمايتها وتركوها مباحة كالمرفقة على الحسابات الشخصية لوسائل التواصل الاجتماعي. ومن حيث المسؤولية الجنائية فلا يُسأل جنائياً من يقم بتجميع البيانات الشخصية المتروكة على خلاف النوع الأول وهو البيانات الشخصية المحمية إذ يتطلب للحصول عليها بدون ترخيص أو إذن ارتكاب أحد الجرائم المنصوص في قانون مكافحة تقنية المعلومات المصري رقم 175 لسنة 2018م وهو ما يتحقق باختراق نظام

(ب) التقط أو نقل بجهاز من الأجهزة أياً كان نوعه صورة شخص في مكان خاص.
فإذا صدرت الأفعال المشار إليها في الفقرتين السابقتين أثناء اجتماع على مسمع أو مرأى من الحاضرين في ذلك الاجتماع، فإن رضاء هؤلاء يكون مفترضاً". حيث ان الركن المادي لهذه الجريمة إذن يشترط ان يتم التقاط صورة لشخص ما في مكان خاص لقيام الركن المادي لهذه الجريمة بينما مجرد جمع البيانات الشخصية المرفقة على وسائل التواصل الاجتماعي لا يدخل في إطار هذه الجريمة.

[1] د. سليمان عبد المنعم: تراجع مبدأ مادية الجريمة، المرجع السابق، ص35.

معلوماتي أو حاسب إلى أو شبكة معلوماتية[1] من ثم يكون مسؤولاً جنائياً عن تلك الجرائم.

جدير بالذكر أنه من يضطلع بجمع البيانات المباحة أو المتروكة لا يكون بمنأى عن المسؤولية الجنائية في جريمة الانتقام الإباحي عبر تقنية التزييف العميق على وجه الخصوص، إذ يعد بذلك شريكاً في هذه الجريمة في الحالة التي يتعدد فيها الفاعلين، ففي هذه الحالة يكون الفاعل الأصلي هو من يضطلع بتوليد المقطع الجنسي المزيف، أما جامع البيانات الشخصية يكون شريكاً إذ يتقاسم الركن المادي للجريمة مع الفاعل الأصلي، **ولكن هل جلب البيانات الشخصية يعد مساهمة أصلية أم مساهمة تبعية؟** المساهمة

---

[1] ويقصد بالاختراق: الدخول غير المرخص به، أو المخالف لأحكام الترخيص، أو الدخول بأى طريقة غير مشروعة، إلى نظام معلوماتى أو حاسب آلى أو شبكة معلوماتية، وما فى حكمها. وفقا لما نصت عليه المادة الأولى من قانون رقم 175 لسنة 2018م. كما نصت المادة (١٤) على أن "يُعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمدًا، أو دخل بخطأ غير عمدي وبقي بدون وجه حق، على موقع أو حساب خاص أو نظام معلوماتى محظور الدخول عليه.

فإذا نتج عن ذلك الدخول إتلاف أو محو أو تغيير أو نسخ أو إعادة نشر للبيانات أو المعلومات الموجودة على ذلك الموقع أو الحساب الخاص أو النظام المعلوماتى، تكون العقوبة الحبس مدة لا تقل عن سنتين، وغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتى ألف جنيه، أو بإحدى هاتين العقوبتين".

وتناولت المادة (١٥) جريمة تجاوز حدود الحق فى الدخول، والتي نصت على أن "يُعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن ثلاثين ألف جنيه ولا تجاوز خمسين ألف جنيه، أو إحدى هاتين العقوبتين، كل من دخل إلى موقع أو حساب خاص أو نظام معلوماتى مستخدمًا حقًا مخولاً له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول.

الأصلية تعني أن يكون للمساهم دور رئيسي في تنفيذ الجريمة سواء منفرداً حين يضطلع بتنفيذ الجريمة بنفسه ويسمى في هذه الحالة بالفاعل المنفرد، وسواء بالاشتراك مع غيره إذ يقومان بتنفيذ الجريمة معاً ويطلق عليه هذه الحالة في هذه الحالة الفاعل مع غيره. وفي الحالتين تكون هذه المساهمة الأصلية مادية[1]، ورغم أهمية جمع البيانات الشخصية من صور وفيديوهات وتسجيلات صوتية وخلافة إلا أن الفعل الأصلي لجريمة الانتقام الإباحي العميق هو توليد المقطع المزيف من خلال تقنية التزييف العميق، وبالتالي من يضطلع بهذا النوع من التلفيق الرقمي هو الفاعل الأصلي في الجريمة أما من يجوب ليجمع البيانات الشخصية ويقدمها لمنتج الفيديو الجنسي المزيف يُعد مساهماً تبعياً[2] بالمساعدة[3].

المرحلة الثانية من مراحل جريمة الانتقام الإباحي عبر تقنية التزييف العميق – بعد تجميع البيانات الشخصية – هو توليد وإنتاج المقطع الجنسي

---

[1] د. سليمان عبد المنعم: النظرية العامة لقانون العقوبات، المرجع السابق، ص 466.

[2] يقصد بالمساهمة التبعية أو ما يسمى بالاشتراك تعدد الجناة في مرحلة سابقة على تنفيذ الجريمة، ألا وهي مرحلة التفكير في ارتكاب الجريمة والإعداد لها. فالمساهمة التبعية إذن لا تعني القيام بدور رئيسي أو أصلي في تنفيذ الجريمة، وإنما تفيد القيام بدور ثانوي أو تبعي مثل تحريض الفاعل الأصلي للجريمة أو مساعدته أو الاتفاق معه...إلخ. ويطلق على المساهم التبعي "الشريك". د. سليمان عبد المنعم: النظرية العامة لقانون العقوبات، المرجع السابق، ص 474.

[3] يقصد بالمساعدة كفعل من أفعال المساهمة التبعية تقدم كافة صور العون إلى الفاعل الأصلي فيرتكب الجريمة بناء على هذا العون. والمساعدة بذلك أهم صورة للمساهمة التبعية، وهي التي تعطي لها شكل المشروع الإجرامي. ويكون على المساهم في الجريمة عقوبتها وفقا لما نصت عليه المادة 41 من قانون العقوبات المصري بقولها "من اشترك في جريمة فعلية عقوبتا إلا ما استثنى قانوناً بنص خاص".

المزيف، من خلال إدخال ودمج البيانات الشخصية للضحية في خوارزمية معدّة لإحلال تلك البيانات بنظيرتها في المقطع الإباحي، لتحل صورة الضحية محل صورة بطل المقطع الإباحي وكذلك الصوت كذلك قوام الجسد، فضلاً عن الاعتماد على تحسين تركيب البيانات على المقطع الإباحي من خلال الخوارزمية التي تستعين في ذلك بإيماءات وحركات وقسمات الوجه لتجعل المقطع المزيف وكأنه حقيقي. هذا الفعل المركب الذي تقوم به خوارزمية الذكاء الاصطناعي يجعل من يغذيها بالبيانات الشخصية مسؤولاً جنائياً عن المقطع الإباحي المزيف الذي تم إنتاجه، ويعد هو الفاعل الأصلي في الجريمة إذ أن توليد المقطع الجنسي المزيف جريمة مستقلة كما سبق ان أوضحنا، ولا يسأل جنائياً مصمم أو مبرمج تقنية التزييف العميق، حيث إن العبرة في إساءة استخدامها من قبل الفاعل الأصلي إلا إذا كان المصمم أو المبرمج على علم باصطناع المقطع الجنسي المزيف ليكون بذلك شريكاً ومساهماً جنائياً مع الفاعل الأصلي في الجريمة غير أنه يظل وصفه القانوني مساهماً تبعياً بالمساعدة. كما يسأل المبرمج باعتباره مساهماً في الحالة الذي يضطلع فيها بصناعة الخوارزميات المعدّة للتزييف الجنسي العميق بغرض بيعها بمقابل أياً كان نوع المقابل.

جدير بالذكر ان المشرع المصري وضع ضوابط معينة لكل متحكم أو معالج في الفصل الثالث من قانون حماية البيانات الشخصية[1] في الحالة

---

[1] حيث نص الفصل الثالث من قانون حماية البيانات الشخصية على: أولا: التزامات المتحكم

مادة (٤): مع مراعاة أحكام المادة (١٢) من هذا القانون، يلتزم المتحكم بما يأتي:

١ – الحصول على البيانات الشخصية أو تلقيها من الحائز أو من الجهات المختصة بتزويده بها بحسب الأحوال بعد موافقة الشخص المعني بالبيانات، أو في الأحوال المصرح بها قانوناً.

٢ – التأكد من صحة البيانات الشخصية واتفاقها وكفايتها مع الغرض المحدد لجمعها.

٣ – وضع طريقة وأسلوب ومعايير المعالجة طبقا للغرض المحدد، ما لم يقرر تفويض المعالج في ذلك بموجب تعاقد مكتوب.

٤ – التأكد من انطباق الغرض المحدد من جمع البيانات الشخصية لأغراض معالجتها.

٥ – القيام بعمل أو الامتناع عن عمل يكون من شأنه إتاحة البيانات الشخصية إلا في الأحوال المصرح بها قانوناً.

٦ – اتخاذ جميع الإجراءات التقنية والتنظيمية وتطبيق المعايير القياسية اللازمة لحماية البيانات الشخصية وتأمينها حفاظًا على سريتها، وعدم اختراقها أو إتلافها أو تغييرها أو العبث بها قِبل أي إجراء غير مشروع.

٧ – محو البيانات الشخصية لديه فور انقضاء الغرض المحدد منها، أما في حال الاحتفاظ بها لأي سبب من الأسباب المشروعة بعد انتهاء الغرض، فيجب ألا تبقي في صورة تسمح بتحديد الشخص المعني بالبيانات.

٨ – تصحيح أي خطأ بالبيانات الشخصية فور إبلاغه أو علمه به.

٩ – إمساك سجل خاص للبيانات، على أن يتضمن وصف فئات البيانات الشخصية لديه، وتحديد من سيفصح لهم عن هذه البيانات أو يتيحها لهم وسنده والمدد الزمنية وقيودها ونطاقها وآليات محو البيانات الشخصية لديه أو تعديلها وأي بيانات أخرى متعلقة بنقل تلك البيانات الشخصية عبر الحدود ووصف الإجراءات التقنية والتنظيمية الخاصة بأمن البيانات.

١٠ – الحصول على ترخيص أو تصريح من المركز للتعامل مع البيانات الشخصية.

١١ – يلتزم المتحكم خارج جمهورية مصر العربية بتعيين ممثل له في جمهورية مصر العربية وذلك على النحو الذي تبينه اللائحة التنفيذية.

١٢ – توفير الإمكانيات اللازمة لإثبات التزامه بتطبيق أحكام هذا القانون وتمكين المركز من التفتيش والرقابة للتأكد من ذلك.

وفي حال وجود أكثر من متحكم يلتزم كل منهم بجميع الالتزامات المنصوص عليها في هذا القانون، وللشخص المعني ممارسة حقوقه تجاه كل متحكم على حدة.

وتحدد اللائحة التنفيذية لهذا القانون السياسات والإجراءات والضوابط والمعايير الفنية لتلك الالتزامات.

ثانيا: التزامات المعالج

مادة (٥): مع مراعاة أحكام المادة (١٢) من هذا القانون، يلتزم معالج البيانات الشخصية بما يأتي:

١ – إجراء المعالجة وتنفيذها طبقاً للقواعد المنظمة لذلك بهذا القانون ولائحته التنفيذية ووفقًا للحالات المشروعة والقانونية وبناءً على التعليمات المكتوبة الواردة إليه من المركز أو المتحكم أو من أي ذي صفة بحسب الأحوال، وبصفة خاصة فيما يتعلق بنطاق عملية المعالجة وموضوعها وطبيعتها ونوع البيانات الشخصية واتفاقها وكفايتها مع الغرض المحدد له.

٢ – أن تكون أغراض المعالجة وممارستها مشروعة، ولا تخالف النظام العام أو الآداب العامة.

٣ – عدم تجاوز الغرض المحدد للمعالجة ومدتها، ويجب إخطار المتحكم أو الشخص المعني بالبيانات أو كل ذي صفة، بحسب الأحوال، بالمدة اللازمة للمعالجة.

٤ – محو البيانات الشخصية بانقضاء مدة المعالجة أو تسليمها للمتحكم.

٥ – القيام بعمل أو الامتناع عن عمل يكون من شأنه إتاحة البيانات الشخصية أو نتائج المعالجة إلا في الأحوال المصرح بها قانوناً.

٦ – عدم إجراء أي معالجة للبيانات الشخصية تتعارض مع غرض المتحكم فيها أو نشاطه إلا إذا كان ذلك بغرض إحصائي أو تعليمي ولا يهدف للربح ودون الإخلال بحرمة الحياة الخاصة.

٧ – حماية وتأمين عملية المعالجة والوسائط والأجهزة الإلكترونية المستخدمة في ذلك وما عليها من بيانات شخصية.

٨ – عدم إلحاق أي ضرر بالشخص المعني بالبيانات بشكل مباشر أو غير مباشر.

٩ – إعداد سجل خاص بعمليات المعالجة لديه، على أن يتضمن فئات المعالجة التي يجريها نيابة عن أي متحكم وبيانات الاتصال به ومسئول حماية البيانات لديه، والمدد

التي يضطلع فيها أحدهم بمعالجة البيانات الشخصية التي يسيطر عليها وإلا كان مسؤولاً جنائياً عن مخالفتها.

أما المرحلة الثالثة والتي تتحقق بها دافع الانتقام لدى الجاني، هي مرحلة إظهار المقطع الجنسي المزيف، من خلال أي وسيلة تحقق هذا

الزمنية للمعالجة وقيودها ونطاقها وآليات محو البيانات الشخصية لديه أو تعديلها، ووصفًا للإجراءات التقنية والتنظيمية الخاصة بأمن البيانات وعمليات المعالجة.

١٠ – توفير الإمكانيات لإثبات التزامه بتطبيق أحكام هذا القانون عند طلب المتحكم وتمكين المركز من التفتيش والرقابة للتأكد من التزامه بذلك.

١١ – الحصول على ترخيص أو تصريح من المركز للتعامل على البيانات الشخصية.

١٢ – يلتزم المعالج خارج جمهورية مصر العربية بتعيين ممثل له في جمهورية مصر العربية وذلك على النحو الذي تبينه اللائحة التنفيذية.

وفي حال وجود أكثر من معالج، يلتزم كل منهم بجميع الالتزامات المنصوص عليها في هذا القانون وذلك في حال عدم وجود عقد يحدد التزامات ومسئوليات كل منهم بوضوح.

وتحدد اللائحة التنفيذية لهذا القانون السياسات والإجراءات والضوابط والشروط والتعليمات والمعايير القياسية لتلك الالتزامات.

ثالثا: شروط المعالجة

مادة (٦): تعد المعالجة الإلكترونية مشروعة وقانونية في حال توفر أي من الحالات الآتية:

١ – موافقة الشخص المعني بالبيانات على إجراء المعالجة من أجل تحقيق غرض محدد أو أكثر.

٢ – أن تكون المعالجة لازمة وضرورية تنفيذًا لالتزام تعاقدي أو تصرف قانوني أو لإبرام عقد لصالح الشخص المعني بالبيانات، أو لمباشرة أي من إجراءات المطالبة بالحقوق القانونية له أو الدفاع عنها.

٣ – تنفيذ التزام ينظمه القانون أو أمر من جهات التحقيق المختصة أو بناءً على حكم قضائي. ٤ – تمكين المتحكم من القيام بالتزاماته أو أي ذي صفة من ممارسة حقوقه المشروعة، ما لم يتعارض ذلك مع الحقوق والحريات الأساسية للشخص المعني بالبيانات.

الإظهار ولعلّ أهمها النشر على الإنترنت، ليكون ناشر هذا المقطع مسؤولا جنائياً عن جريمة نشر محتوى معلوماتي غير مشروع وفقا لما نصّت عليه المادة 25 من قانون مكافحة تقنية المعلومات المصري 175 لسنة 2018م[1]. والنشر بهذه الصورة مفاده إطلاع الجمهور على مضمون المحتوى بحيث يكون متاحاً لهم[2]. وحتى نكون أكثر تفصيلاً يتعين علينا تحديد المسؤول جنائياً عن جرائم النشر عبر المواقع الإلكترونية تارة وعبر وسائل التواصل الاجتماعي تارة أخرى.

فبالنسبة لنشر المقطع الإباحي المزيف على المواقع الإلكترونية تقوم المسؤولية الجنائية للناشر بدايةً وهو أمر بدهي، إلا ان المسؤولية الجنائية قد تمتد لمدير الموقع الإلكتروني، وقد عرّفت المادة الأولى من قانون مكافحة

---

[1] حيث نصت المادة (٢٥) على أن "يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من اعتدى على أى من المبادئ أو القيم الأسرية فى المجتمع المصرى، أو انتهك حرمة الحياة الخاصة أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع إلكترونى لترويج السلع أو الخدمات دون موافقته, أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخباراً أو صوراً وما فى حكمها، تنتهك خصوصية أى شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة. كما نصت المادة (٢٦) على أن "يعاقب بالحبس مدة لا تقل عن سنتين ولا تجاوز خمس سنوات وبغرامة لا تقل عن مائة ألف جنيه لا تجاوز ثلاثمائة ألف جنيه أو بإحدى هاتين العقوبتين كل من تعمد استعمال برنامج معلوماتى أو تقنية معلوماتية فى معالجة معطيات شخصية للغير لربطها بمحتوى منافٍ للآداب العامة، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه".

[2] د. أشرف جابر سيد: مسئولية مقدمي خدمات الإنترنت عن المضمون الإلكتروني غير المشروع، مجلة حقوق حلوان للدراسات القانونية والاقتصادية، العدد 22، 2010م، ص ٢٦ وما بعدها.

جرائم تقنية المعلومات المصري، مدير الموقع بأنه: كل شخص مسئول عن تنظيم أو إدارة أو متابعة أو الحفاظ على موقع أو أكثر على الشبكة المعلوماتية، بما في ذلك حقوق الوصول لمختلف المستخدمين على ذلك الموقع أو تصميمه أو توليد وتنظيم صفحاته أو محتواه أو المسئول عنه. ولقد نصت المادة ٢٧ من القانون ذاته على معاقبة كل من أنشأ أو أدار أو استخدم موقعاً أو حساباً خاصاً على الشبكة المعلوماتية يهدف إلى ارتكاب أو تسهيل ارتكاب جريمة معاقب عليها قانوناً، وبالتالي إذا أنشأ مدير الموقع الإلكتروني مسؤول جنائياً عن المحتوى غير المشروع باعتباره جريمة نص عليها القانون في مواده 25 و26. ويعد مدير الموقع الشخص المسئول عن إدارة المواقع التي تقوم بتقديم الخدمة لمستخدم شبكة الإنترنت، وعن المعلومات التي تمر عبر الشبكة، وبالتالي تكون له سلطة فعلية لمراقبة المعلومات التي يتم بثها، بما يعني أن المقطع الجنسي المزيف كان محل تقدير سابق وفحص من جانبه قبل نشره للجمهور[1]. ومن ثم فإنه يسأل جنائياً عن المعلومات غير المشروعة أو المجرمة لا سيما التزييف الإباحي العميق التي تظهر على شبكة المعلومات الدولية عبر محطة الخدمة التي

[1] د. احمد عبد اللاه المراغي: المسئولية الجنائية لمقدمي خدمات الإنترنت، دراسة تحليلية خاصة لمسئولية مزودي خدمات الاتصالات الإلكترونية، مجلة حقوق حلوان للدراسات القانونية والاقتصادية، ص198، على الرابط التالي بتاريخ دخول 2022/8/18، الساعة 3:20م

https://mklse.journals.ekb.eg/article_229442_6f7598aebf816ee2c6667d10f83ae504.pdf

يُشرف عليها. ومكمن المسئولية هنا مرجعه توافر القدرة الفعلية لديه في السيطرة والتحكم في المراسلات والمعلومات والبيانات قبل بثها[1].

وإذا كان ناشر مقطع الفيديو الإباحي المزيف ومدير الموقع مسؤولون جنائياً **فهل تمتد المسؤولية الجنائية لمقدمي الخدمة؟** بيد أن لاستخدام شبكة الإنترنت لابد من وجود ضلعان متماثلان وهما المزود[2] والمستخدم[3] وقد تزيد تلك الأضلع بزيادة الخدمات، فإن الأمر أثار إشكاليات عديدة خاصة وأن للمزود عدّة أوجه، فالوجه الأساسي باعتباره مزوداً أو مُقدماً لخدمة الإنترنت[4] يقتصر دوره فيه على تمكين مستخدمي الإنترنت من الدخول أو الوصول إلى المواقع دون افتراض علمه بالمحتوى المنشور من ثم لا يُسأل جنائياً لعدم علمه بالمحتوى، وقد يتعهد مقدم خدمة الإنترنت بالإيواء

---

[1] د. أحمد مبروك أحمد مبروك: الجرائم الناتجة عن العمل الإعلامي، رسالة دكتوراه، جامعة حلوان، كلية الحقوق، 2019، ص ١٣٢.

[2] ويطلق عليه مقدم الخدمة، وفقاً للمادة الأولى من قانون مكافحة تقنية المعلومات المصري 175 لسنة 2018م هو أي شخص طبيعي أو اعتباري يزود المستخدمين بخدمات تقنيات المعلومات والاتصالات، ويشمل ذلك من يقوم بمعالجة أو تخزين المعلومات بذاته أومن ينوب عنه في أي من تلك الخدمات أو تقنية المعلومات.

[3] المستخدم: هو كل شخص طبيعى أو اعتبارى، يستعمل خدمات تقنية المعلومات أو يستفيد منها بأى صورة كانت. وفقا للمادة الأولى من قانون مكافحة تقنية المعلومات المصري 175 لسنة 2018م.

[4] د. محمد عرسان أبو الهيجا ود. علاء الدين فواز الخصاونة، المسؤولية التقصيرية لمزودي خدمات الإنترنت عن المحتوى غير المشروع، مجلة الشريعة والقانون، جامعة الإمارات العربية المتحدة، مدينة العين، دولة الإمارات العربية المتحدة، العدد الثاني والأربعون، إبريل ٢٠١٠م، ص ٢٠ وما يليها.

واستضافة الموقع الإلكتروني[1]، ليكون بمثابة مؤجر بمقابل لمكان على الشبكة للزبون الذي ينشر ما يريد من محتوى[2]. وإن كان الظاهر أن متعهد الإيواء يقتصر دوره على تقديم مساحة على الشبكة للغير الذي يقوم بتقديم المحتوى عليها، إلا أن هذا لا يعفيه من المسئولية الجنائية إذا ثبُت علمه الفعلي بالمضمون غير المشروع للموقع الذي يؤويه لا سيما المقطع الإباحي المزيف فإذا ثبُت علمه به فإن ذلك يستتبع قيام مسئوليته[3]. وبالتالي مسئولية متعهد الإيواء تتقرر بحسب القواعد العامة للمسئولية الجنائية[4]. فيمكن اعتباره شريكاً بالمساعدة لمتعهد الخدمة أو متعهد الوصول إذا قدم إليه الوسائل الفنية التي تمكّنه من ارتكاب الجريمة وهو يعلم بالنشاط غير

---

[1] حدة أبو خالفة: النظام القانوني لمتعهد الإيواء عبر الإنترنت في القانون الجزائري والأردني، دراسات، علوم الشريعة والقانون، المجلد 45، العدد 4، ملحق ٢، ٢٠١٨م.

Ch. VERDURE: Les hébergeurs de sites web: victimes ou régulateurs de la société de l'information, ,DCCR,nr68-2005, p. 38.

[2] د. أحمد مبروك أحمد مبروك: الجرائم الناتجة عن العمل الإعلامي، المرجع السابق، ص ١٢٨.

Cholet Sylvie: La responsabilité du fournisseur d'hébergement, Paries, février 2001 p. 2, sur Le site: amdm. Free. Fr/Responsabilite_des_hebergeurs. Htm, feral – Schuhl Christiane Cyber droit, le droit à l'épreuve de L'internet, 3 éd., Dunod, paris, 2002, p. 130.A. PILETTE: La directive, commerce électronique: un bref commentaire, A & M., 2001, p. 39.

[3] د. جميل عبد الباقي الصغير: الإنترنت والقانون الجنائي، دار النهضة العربية، القاهرة، 2002م، ص 155.

[4] د. جميل عبد الباقي الصغير: الإنترنت والقانون الجنائي، المرجع السابق، ص 157.

المشروع للفاعل الأصلي واتجه مع ذلك إلى تأجير المساحة على الشبكة لمتعهد الخدمة لمساعدته على ممارسة نشاطه غير المشروع[1].

بناء عليه لا مسؤولية جنائية على مقدم الخدمة طالما كان مزوداً لخدمة الإنترنت فقط دون علمه بالمحتوى إذ يقتصر دوره وقتئذ على ربط العميل من خلال الجهاز الخاص به – الحاسب الآلي مثلاً – بشبكة الإنترنت فقط لذا يكون غير مسؤول عن عدم مشروعية ما يقع من العميل، غير أنه يسأل جنائياً في أحوال أخرى نص عليها المشرع المصري في قانون مكافحة جرائم تقنية المعلومات لعام 2018م بالمواد من 30 إلى 33 منه[2]،

---

[1] د. أحمد السيد عفيفي: الأحكام العامة للعلانية في قانون العقوبات، دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠١ – ٢٠٠٢ م، ص 554. د. عبد الرحمن هيكل: الضوابط الجنائية لحرية الرأي، دار النهضة العربية للنشر والتوزيع، القاهرة، 2017، ص ١٢٣. أحمد قاسم فرح: النظام القانوني لمقدمي خدمات الإنترنت، مجلة المنارة للبحوث والدراسات، المجلد التاسع، العدد 13، جامعة آل البيت، الأردن، 2007م، ص 353.

[2] حيث نص (الفصل الخامس) الموسوم ب "المسئولية الجنائية لمقدمى الخدمة" على الاتي: مادة (٣٠): يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسمائة ألف جنيه ولا تجاوز مليون جنيه، أو بإحدى هاتين العقوبتين، كل مُقدم خدمة امتنع عن تنفيذ القرار الصادر من المحكمة الجنائية المختصة بحجب أحد المواقع أو الروابط أو المحتوى المُشار إليه فى الفقرة الأولى من المادة (٧) من هذا القانون. فإذا ترتب على الامتناع عن تنفيذ القرار الصادر من المحكمة، وفاة شخص أو أكثر، أو الإضرار بالأمن القومى، تكون العقوبة السجن المشدد والغرامة التى لا تقل عن ثلاثة ملايين جنيه ولا تجاوز عشرين مليون جنيه، وتقضى المحكمة فضلاً عن ذلك بإلغاء ترخيص مزاولة النشاط.

مادة (٣١): يعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسة آلاف جنيه ولا تجاوز عشرين ألف جنيه، أو بإحدى هاتين العقوبتين، كل مقدم خدمة خالف الأحكام

مفادها امتناعه عن تنفيذ القرار القضائي بحجب أحد المواقع أو الروابط أو المحتوى إذا ما تضمنت على سبيل المثال مقاطع فيديو جنسية مزيفة، إذ تنص المادة 7 من القانون ذاته على ان "لجهة التحقيق المختصة، متى قامت أدلة على قيام موقع يُبث داخل الدولة أو خارجها، بوضع أي عبارات أو أرقام أو صور أو أفلام أو أي مواد دعائية، أو ما في حكمها بما يُعد جريمة من الجرائم المنصوص عليها بالقانون..... أن تأمر بحجب الموقع أو المواقع محل البث، كلما أمكن تحقيق ذلك فنيًا" ومقاطع التزييف الإباحي العميق تدخل في حكم الأفلام والتي تعد جريمة وفقا لما نصت عليه المادة 26 والتي تنص على أن " يعاقب .... كل من تعمد استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية للغير لربطها

الواردة بالبند (٢) من الفقرة أولاً من المادة (٢) من هذا القانون، وتتعدد عقوبة الغرامة بتعدد المجني عليهم من مستخدمى الخدمة.

مادة (٣٢): يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل مقدم خدمة امتنع عن تنفيذ القرار الصادر من جهة التحقيق المختصة بتسليم ما لديه من البيانات أو المعلومات المشار إليها فى المادة (٦) من هذا القانون.

مادة (٣٣): يعاقب بغرامة لا تقل عن خمسة ملايين جنية ولا تجاوز عشرة ملايين جنيه، كل مقدم خدمة أخل بأى من التزاماته المنصوص عليها فى البند (١) من الفقرة (أولاً) من المادة (٢) من هذا القانون. وتضاعف عقوبة الغرامة فى حالة العود، وللمحكمة أن تقضى بإلغاء الترخيص.

ويعاقب بغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائتى ألف جنيه، كل مقدم خدمة خالف أحكام الفقرة (ثانيًا) و(رابعًا) من المادة (٢) من هذا القانون.

ويعاقب بالحبس مدة لا تقل عن ثلاثة أشهر، وبالغرامة التى لا تقل عن مائتى ألف جنيه ولا تجاوز مليون جنيه، كل مقدم خدمة خالف أحكام الفقرة (ثالثًا) من المادة (٢) من هذا القانون.

بمحتوى منافٍ للآداب العامة، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه". وبالتالي إذا امتنع مقدم الخدمة عن حجب المحتوى السابق عد مسؤولا جنائياً عن جريمة الامتناع المرتكبة.

أما بالنسبة لنشر المقطع الإباحي المزيف على وسائل التواصل الاجتماعي فهل تتغير أحكام المسؤولية الجنائية بصدده أم لا؟

وسائل التواصل الاجتماعي هي مجموعة من الخدمات الإلكترونية تكون مصممة بشكل يسمح للمستخدمين بإنشاء ملفات تعريفية خاصة بهم[1]، كما يسمح لهم بالتوصل أو تبادل المحتويات معهم كفيسبوك Facebook وتويتر[2] twitter وغيرهما، فضلاً عن كونها تتيح إنشاء علاقات بين مجموعات أو أكثر من الأشخاص الذين تجمعهم رابطة معينة كالقرابة أو

---

[1] social networking service: An electronic service (usually Web – based) designed to allow users to establish a personal or organizational profile and contact other individuals for the purpose of communicating, collaborating, and/or sharing content with them. Most services allow members to restrict the visibility of their profile information to registered service members only, people on an established list of contacts, or particular groups of service users. Examples include Bebo, Facebook, Twitter, and Buzz from Google.

الموقع الإلكتروني للقاموس:ODLISقاموس

www.abc-clio.com/ODLIS/odlis_s.aspx

تاريخ زيارة الموقع: 2021/12/7، الساعة: 5:48 صباحاً.

[2] قاموس ODLIS: الموقع الإلكتروني للقاموس-www.abc clio.com/ODLIS/odlis_s.aspx

الصداقة أو المهنة أو الاهتمامات المشتركة"[1]. ووسائل التواصل الاجتماعي في الأصل عبارة عن مواقع متاحة مجاناً عبر شبكة الإنترنت، بحيث تجذب مستخدمي شبكة الإنترنت للانضمام إلى عضويتها من أجل التواصل بين الأعضاء في عالم افتراضي[2]، حيث تتيح لهم تبادل الآراء والأفكار ووجهات النظر في شتى المجالات والموضوعات، إذ يكون للمستخدم – العضو – حرية الدخول والخروج وتكوين صفحته الشخصية وتدوين ما يرغب عليها ومشاركة الآخرين المحتوى أو التعليق على ما يقومون بنشره بأي وسيلة تعبير متاحة كتابة[3] أو صورة أو فيديو أو رموز تعبيرية[4].

تقع جرائم النشر على وسائل التواصل الاجتماعي من خلال إرفاق المقطع الجنسي المزيف سواء من على الحاسب الآلي أو الهاتف في اللحظة التي يتوفر فيها اتصال بشبكة الإنترنت، ويكون الناشر أو المستخدم الذي يرفق المقطع الجنسي المزيف سواء على حسابه الشخصي أو داخل مجموعات أو على الصفحات العامة المسموح بالنشر فيها فاعلاً أصلياً في

---

[1] د. أشرف جابر سيد، الجوانب القانونية لمواقع التواصل الاجتماعي، دار النهضة العربية، القاهرة، ٢٠١٣م، ص 5.

[2] د. حوراء موسى عبد الرسول موسى: الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، دراسة مقارنة، المرجع السابق، ص28.

[3] تعرف الكتابة الإلكترونية وفقاً لأحكام المادة (1) من قانون رقم (١٥) لسنة ٢٠٠٤م بتنظيم التوقيع الإلكتروني وبإنشاء هيئة تنمية صناعة تكنولوجيا المعلومات بأنها: "كل حروف أو أرقام أو رموز أو أي علامات أخرى تثبت على دعامة إلكترونية أو رقمية أو ضوئية أو أية وسيلة أخرى مشابهة وتعطي دلالة قابلة للإدراك".

[4] د. محمد سامي عبد الصادق، شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، دار النهضة العربية، القاهرة، جمهورية مصر العربية، ٢٠١٦م، ص 5 وما يليها.

جريمة نشر محتوى معلوماتي غير مشروع، أما إعادة النشر والتي تتوفر كخاصية في بعض وسائل التواصل الاجتماعي تدعو للتساؤل! فقانون مكافحة تقنية المعلومات المصري لم يجرّم صورة إعادة النشر مستقلّة فيما يتعلق بالمحتوي المعلوماتي غير المشروع، ولكن الفرض لا يخلو من أحد أمرين، إما أن ينسخ المستخدم الفيديو الجنسي المزيف ليقوم بنشره بواسطة حسابه الخاص فيعد فاعلاً أصلياً آنذاك عن جريمة نشر، وإما أن يعيد نشر المقطع الجنسي المزيف فيكون مساهماً تبعياً في جريمة المحتوى المعلوماتي غير المشروع وخاصية إعادة النشر تقتضي أن يظهر اسم حساب كلا المستخدمين الأول الذي نشر المقطع الجنسي والثاني الذي أعاد نشره وليس أحدهما، ويأخذ من يضع إعجاباً على منشور الفيديو الجنسي المزيف حكم المساهم التبعي[1]، ولا يجوز التذرع بوجوب عدم إنزال العقاب على مُعيد النشر أو الذي يضع إعجاباً على الفيديو الجنسي المزيف لعدم وجود هذه المفردات في نصيّ المادة 25 و26 من قانون مكافحة تقنية جرائم المعلومات 2018، والاكتفاء بمصطلح نشر فقط، وإلا يكون المركز القانوني لمعيد

---

[1] ويرى البعض خلافا لرأينا السابق أن الإعجاب لا يضطلع منفرداً لقيام المسؤولية الجنائية، إذ يمكن أن يحدث الإعجاب من غير قصد نتيجة تصفح الشاشة بالإصبع إن كان تصفح وسيلة التواصل الاجتماعي تلك من خلال جهاز لوحي، بالتالي فإن التفضيل أو الإعجاب بحد ذاته لا يعد جريمة ما لم تكن هناك لصوص تجرم الإعجاب أو تفضيل محتوى مجرم باعتباره تأييداً للمحتوى، إذ لا يمكن تجريم سلوكيات بمنأى عن أهم قاعدة في القانون الجنائي ألا وهي قاعدة أو مبدأ الشرعية التي تنص على أن لا جريمة ولا عقوبة إلا بنص، بالتالي فإن اعتبار التفضيل أو الإعجاب بمشاركة توضع في قائمة التفضيلات في عداد التأييد المعاقب عليه؛ إنما في ذلك توسعاً للتجريم وتحميل النصوص القانونية الجنائية ما لا تحتمل. د. حوراء موسى عبد الرسول موسى: الجرائم المرتكبة عبر وسائل التواصل الاجتماعي، دراسة مقارنة، المرجع السابق، ص391.

النشر أو المعجب الذي يُظهِر ذات المحتوى غير المشروع وينشطّه ويجعل منه مدى أوسع للمشاهدة أفضل من المركز القانوني للناشر كفاعل أصلي وهو أمر غير مستساغ عقلاً، كما إن القواعد العامة في المساهمة الجنائية قابلة للتطبيق في حالة إعادة النشر أو الإعجاب ليكون بذلك معيد النشر أو المعجب مساهمان تبعيان بالمساعدة ولا يقدح في ذلك أن الجريمة الأصلية وقعت بالفعل مما يصعب معه تصور المساهمة لكونها لاحقة على وقوع الجريمة لاعتبارها من الجرائم المستمرة .

تقوم المسؤولية الجنائية كذلك عن جريمة النشر على وسائل التواصل الاجتماعي إذا ساهم في ارتكابها أكثر من شخص، فالجريمة متعددة الأفعال إذا أتى أحداً عملاً من الأعمال المكونة لها فلا تترتب المسؤولية عنها إلا بانضمام تلك الأفعال سوياً، ومثال على ذلك قيام أحد الأشخاص بإنشاء حساب مستخدم عبر أي من وسائل التواصل الاجتماعي وإعداد محتوى يتضمن المقطع الجنسي المزيف، ثم يقوم شخص آخر بالضغط على خيار نشر المحتوى عبر ذات وسيلة التواصل الاجتماعي من خلال ذات حساب المستخدم الذي قام الأول بإعداد المحتوى فيه، فنظراً لوجود صلة قانونية تجمع كلا الشخصين فإن كل منهما يسأل عن فعله بجانب فعل الآخر[1]، إذ

---

[1] "قد يحدد القانون الركن المادي في بعض الجرائم بحيث يقوم على عملين أو أكثر، لا يكفي كل منهما على حده لقيام الجريمة، وهذه هي صورة الجريمة المركبة، في "1" الجرائم نجد الصفة غير المشروعة موزعة على هذه الأعمال بحيث يكمن في كل منها نصيب من عدم المشروعية، وهذه الأعمال تتعادل من حيث أهميتها في تكوين الجريمة مما يقتضي اعتباره مساهماً أصلياً، ويسأل عن النتيجة التي تحققت بناء على مجموع نشاطه ونشاط المساهمين معه كما لو كان قد ارتكبها وحده". د. فوزية عبد الستار، شرح قانون العقوبات القسم الخاص، المرجع السابق، ص ١٩١.

يفترض في هذه الحالة أن كل منهما يسأل عن الجريمة التي لم تتم بفعله وحده إنما تمت بمجموع الأفعال التي ارتكبت في سبيلها، إذ تقوم المسؤولية الجنائية لكل منهما استناداً على أن امتداد خطيئة كل منهما إلى جميع الأفعال التي ترتكب في سبيل الجريمة[1].

كما يُسأل جنائياً كذلك من يُسخر غيره أو يستعمله بأية وسيلة لتنفيذ الفعل المكون للجريمة وكان هذا الشخص الأخير غير مسؤول عنها جنائياً لأي سبب كأن يكون دون السابعة من عمره ويُطلَب منه نشر المقطع الجنسي المزيف عبر أحد وسائل التواصل الاجتماعي بالضغط على زر النشر.

تمتد المسؤولية الجنائية عن جريمة نشر مقطع فيديو جنسي مزيف باعتبارها أحد تطبيقات جرائم المحتوي المعلوماتي غير المشروع للشخص الاعتباري كذلك[2]، إلا أنه يشترط أن ترتكب الجريمة من الأشخاص

---

[1] د. فوزية عبد الستار، المساهمة الجنائية الأصلية، دار النهضة العربية، القاهرة، 1967م، ص ١٨٢.

[2] المسئولية الجنائية للشخص الاعتبارى نص عليها في المواد التالي من القانون رقم 175 لسنة 2018م، مادة (٣٥): يعاقب بالحبس مدة لا تقل عن ثلاثة أشهر وبغرامة لا تقل عن ثلاثين ألف جنية ولا تزيد عن مائة ألف جنية أو بإحدى هاتين العقوبتين، كل مسئول عن الإدارة الفعلية لأي شخص اعتبارى، إذا تعرض الموقع أو الحساب الخاص أو البريد الإلكترونى أو النظام المعلوماتى المخصص للكيان الذي يديره، لأي جريمة من الجرائم المنصوص عليها فى هذا القانون، ولم يبلغ بذلك الجهات المختصة وقت علمه بالجريمة.

مادة (٣٦): فى الأحوال التى ترتكب فيها أى من الجرائم المنصوص عليها فى هذا القانون، باسم ولحساب الشخص الاعتبارى، يعاقب المسئول عن الإدارة الفعلية إذا ثبت علمه بالجريمة أو سهل ارتكابها تحقيقاً لمصلحة له أو لغيره بذات عقوبة الفاعل الأصلى.

الطبيعيين باسم ولحساب الشخص الاعتباري[1]، أي يشترط أن يكون الفاعل الذي ارتكب الجريمة قد انصرفت نيته إلى التصرف باسم ولحساب الشخص الاعتباري لا بصفته الشخصية، وذلك لتحقيق أهداف ومصالح هذا الشخص الاعتباري، بالتالي لو ارتكب السلوك الإجرامي وهو نشر المقطع الجنسي المزيف من قبل أحد العاملين وليس من قبل ممثل الشخص الاعتباري؛ فلا تقوم حينها المسؤولية الجنائية للشخص الاعتباري، إنما يُسأل العامل عن جريمته دون مساءلة الشخص الاعتباري، أضف إلى ذلك جواز قيام المسؤولية في حق كل منهما الممثل والشخص الاعتباري، إذ لا يترتب على تقرير مسئولية الإدارة الفعلية للشخص الاعتبارى استبعاد المسئولية الجنائية للأشخاص الطبيعيين الفاعلين الأصليين أو الشركاء عن ذات الوقائع التى تقوم بها الجريمة[2].

وجب التنويه أن كافة أسباب الإباحة لا يستفيد بها الفاعل الأصلي أو المشارك في جريمة نشر أو إعادة نشر المقطع الجنسي المزيف على وسائل التواصل الاجتماعي لخصوصية هذه الجريمة التي تتعارض مع مضمون الدفاع الشرعي وأداء الواجب، وحق النشر والأخبار والنقد، والقذف

وللمحكمة أن تقضى بإيقاف ترخيص مزاولة الشخص الاعتبار للنشاط مدة لا تزيد على سنة، ولها فى حاله العود أن تحكم بإلغاء الترخيص أو حل الشخص الاعتبارى بحسب الأحوال، ويتم نشر الحكم فى جريدتين يوميتين واسعتى الانتشار على نفقة الشخص الاعتبارى.

[1] يقصد بممثلي الشركات هم الأشخاص الطبيعيين الذين يملكون حق التصرف القانوني بناء على نص لقانون أو اتفاقية لاسم وحساب الشخص الاعتباري.

[2] وفق ما نصت عليه المادة (٣٧) من القانون رقم 175 لسنة 2018م.

المباح أو استعمالاً لحق أو ممارسة الألعاب الرياضية، أو رضا المجني عليه والتي تتطلب للاستفادة منها سلوكا مادياً لا تعبيرياً.

أخيراً ربما لا تثور إشكالية إذا كان للعنصر البشري تدخلاً في توليد واصطناع الفيديو الجنسي الإباحي باستخدام تقنية التزييف العميق ونشره إذ تسند إليه الجريمة باعتبار أن الإنسان وفقا للقواعد العامة هو محل المسؤولية الجنائية[1]، والركن الجوهري الذي تقوم عليه المسؤولية الجنائية هو الخطأ[2]، الناتج عن إرادة واعية، سواء كانت تلك الإرادة إيجابية، وهي تلك التي تُحدث تغيراً في العالم الخارجي[3]، أو من خلال اتخاذ مسلك سلبي[4]. غير إن الإشكالية تكمُن في **مدى صلاحية تطبيقات التزييف العميق كأحد كيانات**

---

[1] فالقاعدة العامة تقضي بألا يسأل إلا الإنسان وما يعزز ذلك مفهوم المسؤولية الجنائية، والحقيقة أن لها مفهومان: الأول مجرد والثاني واقعي، ويُراد بالمفهوم الأول صلاحية الشخص لأن يتحمل تبعة سلوكه، وهنا نجد المسؤولية صفة في الشخص أو حالة تلازمه سواء وقع منه ما يقتضي المساءلة أو لم يقع منه شيء. ويُراد بالمفهوم الثاني (الواقعي) تحميل الشخص تبعة سلوك صدر منه حقيقة، وهنا المسؤولية ليست مجرد صفة أو حالة قائمة بالشخص بل هي جزاء أيضاً، وهذا المفهوم يحتوي على المفهوم الأول لأنه لا يتصور تحميل شخص تبعة عمله المجرم بخضوعه للجزاء المقرر لفعله في قانون العقوبات. د. عوض محمد: قانون العقوبات، القسم العام، المرجع السابق، ص145. د. محمود نجيب حسني: شرح قانون العقوبات القسم العام، النظرية العامة للجريمة، النظرية العامة للعقوبة والتدبير الاحترازي، دار النهضة العربية، القاهرة، الطبعة الثامنة، 2016م، ص572.

[2] جندي عبد الملك: الموسوعة الجنائية، دار إحياء التراث العربي، بيروت، 1976، ص65.

[3] د. سليمان عبد المنعم: النظرية العامة لقانون العقوبات، المرجع السابق، ص398.

[4] د. محمود نجيب حسني: جرائم الامتناع والمسئولية الجنائية عن الامتناع، دار النهضة العربية، القاهرة، 1986م، ص1 وما بعدها.

الذكاء الاصطناعي محلاً للمسؤولية الجنائية؟ وبخاصة في الحالة التي يضطلع فيها منفرداً بإنتاج وتوليد المقطع الجنسي المزيف من تلقاء نفسه دون تدخلاً بشرياً كما لو كانت التقنية معدة للاستخدام الفني والسينما وأنتجت عن طريق الخطأ مقطعاً جنسياً مزيفاً لأحد الفنانات؟

بداية لا يوجد نص جنائي يعاقب كيانات الذكاء الاصطناعي استقلالاً أو يقرر المسؤولية الجنائية لهم حتى الآن، رغم مساعي الاتحاد الأوروبي لوضع قواعد ناظمة لهذه الكيانات[1]، أما الفقه فقد انقسم على نفسه، فمنهم من لم يعترف بالمسؤولية الجنائية نظراً لعدم إمكان ذلك لأن كيانات الذكاء الاصطناعي لا يتوفر لها الأهلية المطلوبة والإدراك لإسناد الفعل المؤثم إليها فهي مجرد وسائل، فضلاً عن عدم جواز توقيع العقوبات الجنائية عليه لعدم صلاحية تحقيق غرضها، أما الجانب الآخر زعم إمكانية مساءلة كيانات الذكاء الاصطناعي جنائياً وعلّلوا وجهة نظرهم بأن المسؤولية الجنائية لا تقتصر عن الإنسان دون سواه وإلا ما كان لمسؤولية الشخص الاعتباري أي قيمة، كما أن أصبح هناك ضرورة للاعتراف بمسؤولية كيانات الذكاء الاصطناعي لمعاصرة التطور التكنولوجي اللحظي وبخاصة ذات تقنيات التعلم العميق إذ أصبحت تحل محل الإنسان في تفكيرها المجرد

---

[1] القواعد الأوربية في القانون المدني للإنسآلة"، والتي اعتمدها البرلمان الأوروبي في 2017/1/16م، لتضع قواعد قانونية تتعلق بعمل هذه "الكائنات" كذلك تحديد المركز القانوني لهذه الروبوتات، وواقع الشخصية القانونية لها، بما في ذلك وضع تعريف أوروبي مشترك لفئات الروبوتات الذكية والمستقلة. د. محمد عرفان الخطيب: المركز القانوني للإنسآلة (Robots)، الشخصية والمسؤولية، دراسة تأصيلية مقارنة، قراءة في القواعد الأوروبية للقانون المدني للإنسآلة لعام 2017م، مجلة كلية القانون الكويتية العالمية، السنة 6، العدد 4، العدد التسلسلي 24، ربيع الأول/ربيع الثاني 1440هـ، ديسمبر 2018م، ص99، هامش رقم6.

واتخاذ القرارات المستقلة، كما أن الجزاءات الجنائية يمكن أن تتغير بما يتناسب مع طبيعة كيانات الذكاء الاصطناعي كتلك التي يتم توقيعها علي الأشخاص الاعتبارية[1].

أما من الناحية الواقعية فالخطأ الناتج عنه توليد مقطع جنسي مزيف لابد أن ينسب لشخص ما طبيعي أو معنوي حتى يصلح قيام المسؤولية الجنائية في مواجهته، كالمبرمج أو صانع الخوارزمية أو مدخل البيانات أو أي شخص آخر، إلا أن الجريمة في هذه الحالة لا تكون جريمة عمدية وإنما جريمة خطئية نتيجة إهمال أحدهم أو عدم اكتراثه لخطوة من خطوات بناء الخوارزمية أو غيرها من صور الخطأ التي نصّ عليها القانون كرعونته أثناء تنفيذها. وهذا لم يضعه المشرع المصري في الحسبان والذي حدد القصد الجنائي العمدي دون سواه في جريمة نشر المحتوى المعلوماتي غير المشروع، غير أنه من الوارد أن تحدث الجريمة بخطأ، الأمر الذي لا يجوز معه تماثل العقوبة في الحالتين إذ أن القصد الجنائي أحد عوامل تخفيف أو تشديد العقوبة، وكان حريّ على المشرع ألا يقصر الجريمة على العمد فقط ليحيلها إلى القواعد العامة، ويعطي للقاضي الجنائي استخلاص هذا القصد وإعمال مبدأ التفريد العقابي لينزل العقوبة الأكثر تناسباً مع الفعل في كل حالة على حدة.

---

[1] في تفصيل وجهتي النظر يرجع إلى د. محمود سلامة عبد المنعم الشريف: المسؤولية الجنائية للإنسآلة: دراسة تأصيلية مقارنة، المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي، مجلد 3 عدد 1 (2021)، على الرابط التالي:
https://journals.nauss.edu.sa/index.php/AJFSFM/article/view/1122

ثانياً: الملاحقة الجنائية لمرتكبي جرائم التزييف الإباحي العميق

لما كانت جريمة الانتقام الإباحي عبر تقنية التزييف العميق من الجرائم العابرة للحدود، فثمة صعوبة ما في ملاحقة مرتكبي هذه الجريمة جنائياَ[1] غير أن تلك الصعوبة تتضاءل إذا كان الجناة بداخل مصر واتُخذ

---

[1] وتزداد الصعوبة أحياناً حال عدم تحديد مؤلف المعلومة أو صاحبها نظراً لاستخدام بعض مستخدمي وسائل التواصل الاجتماعي لأسماء مستعارة لدى قيامهم بنشر أو إعادة نشر المحتوى غير المشروع – المجرم – أو بسب بسبب انتحالهم أسماء للغير أو بسبب قيامهم باستخدام عنوان بروتوكولي وهمي، هذا بالإضافة إلى عدم النص صراحة في بعض النصوص الواردة في التشريعات الخاصة بمكافحة جرائم تقنية المعلومات على إسناد المسؤولية، مما قد يجعل المشتغلين بالقانون غير مستقرين حتى الآن على قواعد إسناد المسؤولية الجنائية عن الجرائم المرتكبة عبر وسائل التواصل الاجتماعي. إلا أنه من خلال هذه المراقبة يمكن لمزود الخدمة عن طريق العنوان البروتوكولي IP أن يتوصل لهوية المتهم في ارتكاب تلك الجرائم، الأمر الذي من شأنه سهولة ملاحقته قضائياً متى طلبت السلطات المختصة بيانات المستخدم. إذ أنه يمكن لمزود خدمات الإنترنت من الناحية النظرية أن يكتشف كل أفعال مستخدم الإنترنت عندما يتصل بالشبكة، ويشمل ذلك: عناوين المواقع التي زارها، ومتى كان ذلك، والصفحات التي اطلع عليها، والملفات التي جلبها، والكلمات التي بحث عنها، والحوارات التي شارك بها، والبريد الإلكتروني الذي أرسله أو استقبله، وفواتير الشراء للسلع التي طلب شراءها، والخدمات التي شارك فيها، لكن تختلف من الناحية الفعلية كمية المعلومات التي يجمعها مزود خدمات الإنترنت عن مستخدم الشبكة باختلاف التقنيات والبرمجيات التي يستخدمها، لم يكن مزود الخدمة يستخدم مزودات (بروكسي) تتسلم وتنظم كل الطلبات، ويستخدم برامج تحسس الرقم الخاص (IP) التي تحلل حركة المرور بتفصيل كبير، فقد لا يسجل سوى البيانات الشخصية للمستخدم، وتاريخ وزمن الاتصال والانفصال عن الشبكة، وبعض البيانات الأخرى، إن معرفة البيانات التفصيلية للمستخدم تجعل الإقدام على الاعتداء الإلكتروني أقل، وذلك لأن بعض الذي يحصل منهم الاعتداء الإلكتروني يتم منهم ذلك بسبب ظنهم أن بياناتهم التفصيلية لا يمكن الاطلاع عليها، فيظن أنه بمجرد دخوله على الشبكة باسم

السلوك المادي أو جزء منه، وتحقّقت كذلك نتائج الجريمة بداخلها وفقاً لمبدأ الإقليمية[1]، وإنما تثار الإشكالية بحق، إذا لم يكن مرتكبوها بداخل الدولة أو تحقق أحد عناصرها خارج الدولة والعنصر الآخر داخلها كأن يتم إنشاء الفيديو المزيف خارج الدولة ثم يتم بثه بداخلها من خلال وسائل الاتصال التكنولوجية الحديثة، **فهل يُمنح الاختصاص للقانون الجنائي المصري وللقضاء بنظر الجرائم المرتكبة عبر تقنية التزييف العميق في هذه الحالة أم لا؟**

لا شك أن تحقق أحد عناصر الركن المادي للجريمة سواء كان الفعل وهو إنشاء الفيديو المزيف أو النتيجة وهو إلحاق الضرر بأحد الأشخاص في مصر أو حتى ارتكاب جزء من الركن المادي فيها[2] يمنح الاختصاص

وهمي تصبح بياناته غير معلومة". فهد عبد الله العبيد العازمي، الإجراءات الجنائية المعلوماتية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ٢٠١٢م، ص ٤٨١ وما يليها.

[1] نقض جنائي مصري، الطعن رقم ١١٠٢٤ لسنة ٨٨ قضائية، الدوائر الجنائية – جلسة 2021/01/13م، على الموقع المرفق بتاريخ دخول 2022/2/10م، الساعة 1:40 مساء:

https://www.cc.gov.eg/judgment_single?id=111646027&&ja=287676

[2] وهذا ما نوهت عنه المادة 3 من القانون رقم 175 لسنة 2018 بقولها "مع عدم الإخلال بأحكام الباب الأول من الكتاب الأول من قانون العقوبات، تسري أحكام هذا القانون على كل من ارتكب خارج جمهورية مصر العربية من غير المصريين جريمة من الجرائم المنصوص عليها من هذا القانون، متى كان الفعل معاقبًا عليه فى الدولة التى وقع فيها تحت أى وصف قانونى، وذلك فى أى من الأحوال الآتية:

١ – إذا ارتكبت الجريمة على متن أى وسيلة من وسائل النقل الجوى أو البري أو المائى، وكانت مسجلة لدى جمهورية مصر العربية أو تحمل علمها.

للقضاء الجنائي المصري بنظر تلك الجريمة ومحاكمة مرتكبيها[1]، وهذا لا يعد مظهرا من مظاهر التوسع في مبدأ الإقليمية إذا ما قورن بمسلك القضاء الفرنسي الذي اعتبر نفسه مختصاً بنظر الجريمة لمجرد تحقق بعض آثارها داخل الإقليم الفرنسي، كما في إحدى جرائم النشر التي وقعت بواسطة صحيفة تم طبعها وتوزيعها في دولة أجنبية، لكن بعضاً من نسخها قد وزع في فرنسا[2]. وإذا ما سلمنا باختصاص القضاء الجنائي المصري في تلك الحالة **فكيف تتم الملاحقة الجنائية للمجرمين في الخارج؟**

بيد أنه تكمُن صعوبة الملاحقة القضائية لمرتكبي الجرائم بواسطة التزييف العميق باعتبارها أحد الجرائم العابرة للوطنية في الحالة التي لم تبرم فيها الدولة معاهدات تسليم مجرمين[3]، وهذه المعاهدات غير موجودة بالفعل

---

٢ – إذا كان المجني عليهم أو أحدهم مصرياً.

٣ – إذا تم الإعداد للجريمة أو التخطيط أو التوجيه أو الإشراف عليها أو تمويلها فى جمهورية مصر العربية.

٤ – إذا ارتكبت الجريمة بواسطة جماعة إجرامية منظمة، تمارس أنشطة إجرامية فى أكثر من دولة من بينها جمهورية مصر العربية.

٥ – إذا كان من شأن الجريمة إلحاق ضرر بأى من موطنى جمهورية مصر العربية أو المقيمين فيها، أو بأمنها أو بأى من مصالحها، فى الداخل أو الخارج.

٦ – إذا وُجد مرتكب جريمة فى جمهورية مصر العربية، بعد ارتكابها ولم يتم تسليمه.

[1] د. سليمان عبد المنعم: النظرية العامة لقانون العقوبات، المرجع السابق، ص65 وما بعدها.

[2] Cass. Crim. 30 Avril 1908, Sirey, 1908, 1, p. 553, note Roux;

[3] يقصد بتسليم المجرمين أو ما يسمى الاسترداد L'extradition مطالبة دولة لأخرى بتسليمها شخصاً ينسب إليه ارتكاب جريمة أو صدر حكم بالعقوبة ضده حتى تتمكن هذه الدولة من محاكمته أو من تنفيذ العقوبة في مواجهته، وذلك باعتبار أنها صاحبة الاختصاص الطبيعي باتخاذ الإجراءات الناشئة عن الجريمة أو تنفيذ العقوبة الصادرة ضد

نظراً لحداثة هذا النوع من الجرائم، وبمفهوم المخالفة لا يعني ذلك ان بمجرد وجود تلك المعاهدات سيكون من اليسير على الدولة ملاحقة الجناة، وإنما ينبغي لتسليمهم من ناحية أولى: أن تكون الجريمة المنسوبة إلى الشخص المطلوب تسليمه من بين الجرائم التي يجوز فيها التسليم، فالجرائم السياسية على سبيل المثال لا يجوز التسليم بصددها، من ثم إذا كان الباعث من انشاء ونشر الفيديو المزيف سياسياً فسيصبح عقبه تجاه ملاحقة الجناة[1]، كما لو زيف أحد الأشخاص خارج الدولة محتوى فيديو لمرشح ما أثناء فترة العملية الانتخابية بغرض التأثير على شعبيته ورسوبه في انتخابات دولة جنسيته.

كما يجب من ناحية ثانية: توافر شروط ازدواج التجريم، فيمتنع التسليم إذا كانت الأفعال المرتكبة عبر تقنية التزييف العميق لا عقاب عليها في قانون الدولة المطلوب منها التسليم[2]، ولكن لا يمنع من توافر شرط ازدواج التجريم أن يكون الفعل معاقباً عليه في قانون كل من الدولتين وإنما تحت وصف قانوني مختلف[3]. وأخيراً يلزم أن تكون هذه الجريمة على درجة

الشخص المطلوب تسليمه. د. سليمان عبد المنعم، الجوانب الإشكالية في النظام القانوني لتسليم المجرمين، دراسة مقارنة، دار المطبوعات الجامعية، الإسكندرية، 2015م، ص57، كذلك د. عبد الفتاح سراج، النظرية العامة لتسليم المجرمين، دراسة تحليلية وتأصيلية، دار النهضة العربية، القاهرة، 1998م، ص13 وما بعدها.

(1) Lemouland, Les critères jurisprudentiels de l'infraction politique, R.S.C. 1988, P. 16.

(2) د. سليمان عبد المنعم: الجوانب الإشكالية في النظام القانوني لتسليم المجرمين، المرجع السابق، ص36.

(3) Conseil d'Etat, 27 Février 1985, Recueil de Conseil d'Etat, p49.

وفي نفس المعنى:

معينة من الجسامة وهذا الشرط متحقق بطبيعة الحال في نوعية الجرائم المرتكبة عبر تقنية التزييف العميق سواء كان الغرض منها الانتقام الاباحي أو التأثير على شفافية ونزاهة العملية الانتخابية أو الإبتزاز الإلكتروني وغيرها من الصور.

تكمُن صعوبة الملاحقة القضائية لمرتكبي جرائم التزييف العميق كذلك في عدم الاعتراف بحجية الأحكام الجنائية الأجنبية، ويستند هذا الفكر إلى مبدأ السيادة القضائية لكل دولة حيث يجب على محاكم كل دولة أن تمتنع عن الاعتراف بحجية للأحكام الصادرة في دولة أخرى لأن الحكم القضائي الجنائي –شأنه شأن التشريع– تعبير عن سيادة الدولة، وفي مصر لا تكتسب الاحكام الأجنبية أدنى حجية فيما تتضمنه من عقوبات أصلية أو غير أصلية. إذ أن إضفاء حجية على مثل هذه الأحكام لا يكون إلا بنص خاص، وليس في القانون المصري ما يفيد ذلك[1]. غير أن مبدأ عدم الإفلات من العقاب يقتضي تذليل العقبات نحو ملاحقة مرتكبو جرائم التزييف العميق والتي من بينها الاعتراف بحجية الأحكام الجنائية الأجنبية.

وقد أسند قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018م للسلطات الاضطلاع بالتعاون الدولى مع نظيراتها بالبلاد الأجنبية فى إطار الاتفاقيات الدولية والإقليمية والثنائية المصدق عليها، أو تطبيق مبدأ المعاملة بالمثل، بتبادل المعلومات بما من شأنه أن يكفل تفادى

Cass. Crim. 15 Juliet 1937, D. P. 1939, 1, p. 60.

[1] د. سليمان عبد المنعم: النظرية العامة لقانون العقوبات، المرجع السابق، ص 107.

ارتكاب جرائم تقنيه المعلومات، والمساعدة على التحقيق فيها، وتتبع مرتكبيها[1].

[1] وفقاً لما نصت عليه المادة 4 من قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018م.

الخاتمة

لا يعاقب القانون الجنائي على الكذب المجرد، فالكذب والتلفيق يدخل في دائرة الأخلاق، إلا أن التكنولوجيا الحديثة أفرزت لنا صوراً من الكذب والتلفيق تؤثر سلبياً على المصالح الجوهرية في المجتمع لاسيما سمعة الإنسان وشرفه واعتباره، فاستعمال تقنية التزييف العميق في تلفيق واقعة جنسية مفبركة لشخص ما لم يرتكبها في الحقيقة بغرض الانتقام منه، أمر يتعين على المشرع أن يتفطّن لها مبكراً حتى يقطع دابر من تسول له نفسه إتيان هذا السلوك المشين.

إن محاولة دمج الجرائم المستحدثة كالتزييف الإباحي العميق ضمن نصوص قانون العقوبات المصري قد يوقعنا في شرك التفسير الموسع للنص الجنائي وهو ما يخالف مقتضى وطبيعة هذا النوع من النصوص القانونية التي يُحرم فيها التفسير الموسع والقياس عليها. ولم يصرّح المشرع المصري رغم حداثة القوانين الجنائية المتعلقة بالجرائم المعلوماتية وحماية البيانات الشخصية بمصطلح "جريمة الانتقام الإباحي العميق" إلا أنه يمكن اعتبارها ضمن تطبيقات جرائم المحتوى المعلوماتي غير المشروع.

جدير بالذكر أنه لا تقتصر مخاطر تقنية التزييف العميق على الصور ومقاطع الفيديو الملفّقة للأشخاص بل يُمكن أن تمتد لتزييف صور الأقمار الصناعية لنشر معلومات خاطئة عن الكوارث الطبيعية مثل الفيضانات وحرائق الغابات أو تغيير حدود دولة معينة وترسيخ ذلك في الأذهان على غير الحقيقة، كذلك للتلاعب بسرد قصص غير حقيقية لأقليات معينة تعاني التعذيب أو الترويع، فضلاً عن تزييف القضايا البيئية المتعلقة بإزالة الغابات في منطقة الأمازون على سبيل المثال.

النتائج

1- الانتقام الإباحي العميق يختلف عن الانتقام الإباحي المحض، فالأول هو تلفيق رقمي لواقعة لم تحدث في الحقيقة باستخدام تقنية التزييف العميق، أما الثاني هو مجرد فضح واقعة حقيقية تم نشرها بدون علم صاحب البيانات.

2- لم ينص المشرع المصري والفرنسي صراحة على تجريم استعمال تقنية التزييف العميق باعتبارها جزء من النموذج القانوني للجريمة على خلاف المشرع الأمريكي في بعض الولايات الذي بادر بوضعه ضمن الأفعال المجرمة.

3- الركن المادي لجريمة الانتقام الإباحي عبر تقنية التزييف العميق يتحقق بتتابع بعض الأفعال لاسيما تجميع البيانات الشخصية ثم معالجتها لتوليد وإنتاج الفيديو وأخيراً إظهاره. غير أن المسؤول جنائياً يتحدد بحسب كل مرحلة من المراحل.

4- استعمل المشرع المصري كلمة "إظهار" في المادة 26 من القانون رقم 175 لسنة 2018م بدلاً من العلانية أو النشر، وحسناً ما فعل، إذ يدخل في مفهوم الإظهار مالا يدخل في مفهوم العلانية كالتراسل الخاص للمقطع الجنسي المزيف.

5- رغم التباين بين الانتقام الإباحي والابتزاز الإلكتروني من حيث ركنه المادي والغرض من إتيان الجريمة كذلك من حيث الوسيلة إلا أنهما قد يجتمعا في الحالة التي ينتج فيها الجاني مقطع جنسي مزيف للضحية بغرض التهديد به وطلب منفعة معينة.

6- غدى يسيراً للأفراد العاديين الاستحواذ على البيانات الشخصية وبخاصة لمستخدمي وسائل التواصل الاجتماعي نظراً لإتاحتها والتي تكون وقوداً لإنتاج المقطع الإباحي المزيف ولا يشترط أن يكون له السيطرة على البيانات الشخصية كالمتحكم أو المعالج.

7- مرحلة التحريف أو التلفيق عبّر عن مدلولها المشرع المصري بـ "المعالجة الإلكترونية" في القانون رقم ١٧٥ لسنة ٢٠١٨ وهي تعد جريمة مستقلة بذاتها كأحد تطبيقات جريمة المحتوى المعلوماتي غير المشروع حتى ولو لم يتم نشر المقطع الجنسي الذي تم تحريفه وتلفيقه في الحالة التي يتم فيها ربط المحتوى بما هو منافي للآداب العامة كما في التزييف الإباحي العميق.

8- الشروع متصور في جريمة التزييف الإباحي العميق بصورتيه التامة في حالة إنتاج المقطع ولكن كان مشوهاً ليفقد معه تحديد الأشخاص فيه، والناقصة في حالة عدم إنتاج المقطع الجنسي المزيف نتيجة لتجاوز أحد الخطوات المتوالية خطأً. أما شراء أو الاشتراك في خوارزميات التزييف العميق، أو حيازة أحد تطبيقاته على الهاتف أو الجهاز الحوسبي، أو مجرد تجميع وحيازة صور للفانين، أو التدريب على كيفية تشغيل برامج التزييف العميق أو غيرها من الأفعال التي لا تعد شروعاً وإنما تدخل في نطاق الأعمال التحضيرية التي لا عقاب عليها.

9- لم يتطلب المشرع المصري قصداً خاصاً لهذه الجريمة بل اكتفى بتوافر القصد العام، وبالتالي يستوي ان يكون إنتاج وتوليد الفيديو المزيف بغرض الانتقام أو بغرض الارتزاق أو بغرض التفاخر بالنفس أو إرضاء شعور غريزي لديه أو غيرها من الأغراض.

10- تمتد العقوبة الجنائية للأشخاص الاعتبارية في الأحوال التي ترتكب فيها جريمة التزييف الإباحي العميق باعتبارها أحد جرائم معالجة المعطيات الشخصية للغير، باسم ولحساب الشخص الاعتباري ويعاقب المسئول عن الإدارة الفعلية إذا ثبت علمه بالجريمة أو سهل ارتكابها تحقيقا لمصلحة له أو لغيره بذات عقوبة الفاعل الأصلي.

11- من يضطلع بجمع البيانات المباحة أو المتروكة لا يكون بمنأى عن المسؤولية الجنائية في جريمة الانتقام الإباحي عبر تقنية التزييف العميق على وجه الخصوص، إذ يعد بذلك شريكاً في هذه الجريمة في الحالة التي يتعدد فيها المساهمين، ففي هذه الحالة يكون الفاعل الأصلي هو من يضطلع بتوليد المقطع الجنسي المزيف.

12- المسؤولية الجنائية عن جريمة نشر المقطع الإباحي المزيف تمتد لمدير الموقع الإلكتروني بالإضافة إلى الناشر، كما إنها قد تمتد لمتعهد الخدمة ومقدم الخدمة في الحالة التي يتحقق لديهم العلم فيها بنشر هذا المحتوى غير المشروع.

13- معيد النشر ومن يضع أعجاباً على المقطع الجنسي المزيف مسؤولون جنائياً باعتبارهم مساهمين تبعيين عن جريمة التزييف الإباحي العميق والذي يعد الناشر هو الفاعل الأصلي فيها باعتبارها من الجرائم المستمرة يتسم نشاطها المادي بطابع الاستمرار.

14- إذا تم إنتاج فيديو جنسي مزيف من خلال برنامج التزييف العميق استقلالا دون علم المبرمج أو المستخدم، تتحول الجريمة من عمدية إلى خطأيه لصعوبة مساءلة برامج التزييف العميق جنائياً كأحد تطبيقات الذكاء الاصطناعي ريثما يكون هناك قواعد جنائية ناظمة لهذه الكيانات.

15- يختص القضاء المصري بنظر جريمة الانتقام الإباحي عبر تقنية التزييف العميق حتى ولو ارتكب أي فعل من الأفعال المكونة للركن المادي للجريمة داخل مصر أو طال ضررها أي شخص بداخلها.

التوصيات

أولاً: من المناسب أن يدرج المشرع المصري مصطلح "التزييف العميق -**Deepfakes**" على الأقل كظرف مشدد للعقوبة الواردة في نص المادة 26 منه، حال استعمال بيانات شخص ما لمحتوى منافٍ للآداب العامة، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه، ليكون العقاب على جريمة الانتقام الإباحي العميق مشدداً.

ثانياً: من المناسب أن يضيف المشرع المصري كلمة "تزييف" ضِمن أغراض العمليات الإلكترونية التي عدّدها في تعريف "المعالجة الإلكترونية" التي تضمنتها المادة الأولى من القانون رقم 175 لسنة 2018م، لأن التزييف هو تخليق وقائع غير حقيقية، فهو مصطلح أدق وأشمل من مجرد الاستنباط أو دمج أو تعديل أو تغيير البيانات التي أوردها المشرع في نص المادة.

ثالثاً: من المناسب أن يستبدل المشرع المصري مصطلح "معطيات شخصية" بـ "بيانات شخصية" اتساقا مع التعريفات التي ذكرها من ناحية ولتوحيد صياغة النص من ناحية أخرى كما استخدمها في المادة 25 من القانون ذاته.

رابعاً: من المناسب أن يجعل المشرع المصري العقوبة وجوبية لا تخييرية في نص المادة 26 من القانون رقم 175 لسنة 2018 وبخاصة حال ارتكاب جريمة التزييف الإباحي العميق.

خامساً: من المناسب أن يضيف المشرع المصري مصطلح "الانتقام الإباحي" للأغراض التي نصّ عليها في المادة 34 من القانون رقم 175 لسنة 2018م وهي الحالات التي يشدد فيها العقاب إذا وقعت الجريمة لتحقيق أحد أغراضها.

سادسا: من المناسب أن يحذف المشرع جملة " كل من تعمد" في نص المادة 26 من القانون رقم 175 لسنة 2018م وذلك لأن من المتصور أن تتحقق جريمة تزييف الإباحي العميق دون عمد سواء عن طريق الخطأ او الإهمال أو الرعونة في التعامل مع برامج الذكاء الاصطناعي.

قائمة المراجع

أولاً: اللغة العربية

1- ابن منظور: لسان العرب، المجلد السادس، باب الواو، ج53، دار المعارف، الإسكندرية.

ثانياً: المراجع القانونية

أ- مراجع عامة

1- جندي عبد الملك: الموسوعة الجنائية، دار إحياء التراث العربي، بيروت، 1976م.

2- ـــــــــــــــ: النظرية العامة لقانون العقوبات، دار المطبوعات الجامعية، الإسكندرية، 2014م.

3- سليمان مرقس: المسؤولية المدنية في تقنينات البلاد العربية، معهد البحوث والدراسات العربية، القاهرة، 1960م.

4- عبد الفتاح سراج: النظرية العامة لتسليم المجرمين، دراسة تحليلية وتأصيلية، دار النهضة العربية، القاهرة، 1998م.

5- عوض محمد: قانون العقوبات، القسم العام، مؤسسة الثقافة الجامعية، الإسكندرية، 2007م.

6- فوزية عبد الستار: شرح قانون العقوبات القسم الخاص، دار النهضة العربية، القاهرة، 1987م.

7- محمد كمال الدين إمام: المسؤولية الجنائية أساسها وتطورها: دراسة مقارنة في القانون الوضعي والشريعة الإسلامية، دار الجامعة الجديدة، الإسكندرية، 2004م.

8- محمود محمود مصطفى: شرح قانون العقوبات، دار النهضة العربية، القاهرة، 1987م.

9- محمود نجيب حسني: شرح قانون العقوبات القسم العام، النظرية العامة للجريمة، النظرية العامة للعقوبة والتدبير الاحترازي، دار النهضة العربية، القاهرة، الطبعة الثامنة، 2016م.

ب- مراجع متخصصة

1-أحمد السيد عفيفي: الأحكام العامة للعلانية في قانون العقوبات، دراسة مقارنة، دار النهضة العربية، القاهرة، ٢٠٠١ – ٢٠٠٢ م.

2-أشرف توفيق شمس الدين: الحماية الجنائية للحق في صيانة العرض، دار النهضة العربية، القاهرة، 2004م.

3-أشرف جابر سيد: الجوانب القانونية لمواقع التواصل الاجتماعي، دار النهضة العربية، القاهرة، ٢٠١٣م.

4- تامر محمد صالح: الابتزاز الإلكتروني، دراسة تحليلية مقارنة، دار الفكر والقانون، المنصورة، 2021م.

5- جلال ثروت: نظم القسم الخاص، جرائم الاعتداء على الأشخاص، دار المطبوعات الجامعية، الإسكندرية، الجزء الأول، 1995م.

6-جميل عبد الباقي الصغير: الإنترنت والقانون الجنائي، دار النهضة العربية، القاهرة، 2002م.

7-حوراء موسى: الجرائم المرتكبة عبر وسائل التواصل الاجتماعي: دراسة مقارنة، دار النهضة العربية، القاهرة، 2018م.

8- سعيد عبد اللطيف حسن: الحماية الجنائية للعرض، دار النهضة العربية، القاهرة، 2004م.

9- السعيد مصطفى السعيد: الأحكام العامة فى قانون العقوبات، مؤسسة المعارف للطباعة والنشر، القاهرة، 1957م.

10- سليمان عبد المنعم: الجوانب الإشكالية في النظام القانوني لتسليم المجرمين، دار المطبوعات الجامعية، الإسكندرية، 2015م.
11- تراجع مبدأ مادية الجريمة، دار المطبوعات الجامعية، الإسكندرية، 2015م.
12- سمير الشناوي: الشروع في الجريمة، دار النهضة العربية للنشر والتوزيع، القاهرة، ١٩٧١م.
13- شريف السيد كامل: المسؤولية الجنائية للأشخاص المعنوية، دار النهضة العربية للنشر والتوزيع، القاهرة، 1997م.
14- عبد الرحمن هيكل: الضوابط الجنائية لحرية الرأي، دار النهضة العربية للنشر والتوزيع، القاهرة، 2017م.
15- عبد الله موسي، أحمد حبيب بلال: الذكاء الاصطناعي، ثورة في تقنيات العصر، المجموعة العربية للتدريب والنشر، القاهرة، الطبعة الأولى، 2019م.
16- عبير أسعد: الذكاء الاصطناعي، دار البداية، القاهرة، الطبعة الأولى، 2017م.
17- فوزية عبد الستار: المساهمة الجنائية الأصلية، دار النهضة العربية، القاهرة، 1967م.
18- ماري شروتر: الذكاء الاصطناعي ومكافحة التطرف العنيف: كتاب تمهيدي، الشبكة العالمية للتطرف والتكنولوجيا GNET، المركز الدولي لدراسة الراديكالية، كينجز كوليدج لندن، بدون سنة نشر.
19- محمد زكي أبو عامر: الحماية الجنائية للعرض، دار النهضة العربية، القاهرة، ١٩٨٦م.

20- محمد سامي عبد الصادق: شبكات التواصل الاجتماعي ومخاطر انتهاك الحق في الخصوصية، دار النهضة العربية، القاهرة، ٢٠١٦م.

21- محمود نجيب حسني: جرائم الامتناع والمسئولية الجنائية عن الامتناع، دار النهضة العربية، القاهرة، 1986م.

22- ـــــــــــــــــ: الحق في صيانة العرض في الشريعة الإسلامية وفي قانون العقوبات المصري، بدون ذكر دار نشر، 1984م.

ثالثاً: الرسائل العلمية

1- أحمد مبروك أحمد مبروك: الجرائم الناتجة عن العمل الإعلامي، رسالة دكتوراه، جامعة حلوان، كلية الحقوق، 2019م.

2- حسني الجندي: نظرية الجريمة المستحيلة في القانون المصري المقارن والشريعة الإسلامية، رسالة دكتوراه، كلية الحقوق، جامعة القاهرة، ١٩٨٠م.

3- حورية محمد عبد الرحيم موسى: أثر وسيلة ارتكاب الجريمة على تشديد العقوبة، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، 2016م.

4- فهد عبد الله العبيد العازمي: الإجراءات الجنائية المعلوماتية، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، جمهورية مصر العربية، ٢٠١٢م.

رابعاً: المجلات والمقالات والمنشورات

1- أحمد عبد اللاه المراغي: المسئولية الجنائية لمقدمي خدمات الإنترنت، دراسة تحليلية خاصة لمسئولية مزودي خدمات الاتصالات

الإلكترونية، مجلة حقوق حلوان للدراسات القانونية والاقتصادية، على الرابط التالي بتاريخ دخول 2022/8/18م، الساعة 3:20مساء
https://mklse.journals.ekb.eg/article_229442_6f7598aebf81 6ee2c6667d10f83ae504.pdf

2- أحمد عبد الموجود زكير: جريمة التزييف الإباحي العميق، دراسة مقارنة، المجلة القانونية، جامعة القاهرة، كلية الحقوق (فرع الخرطوم)، المجلد 11، العدد 7، 2022م.

3- أحمد قاسم فرح: النظام القانوني لمقدمي خدمات الإنترنت، مجلة المنارة للبحوث والدراسات، المجلد التاسع، العدد 13، جامعة آل البيت، الأردن، 2007م.

4- أحمد محمد فتحي الخولي: المسئولية المدنية الناتجة عن الاستخدام غير المشروع لتطبيقات الذكاء الاصطناعي "الديب فيك نموذجاً"، مجلة البحوث الفقهية والقانونية، جامعة الازهر بدمنهور، العدد السادس والثلاثون، أكتوبر 2021م-1443هـ.

5- أشرف جابر سيد: مسئولية مقدمي خدمات الإنترنت عن المضمون الإلكتروني غير المشروع، مجلة حقوق حلوان للدراسات القانونية والاقتصادية، العدد 22، 2010م.

6- آلان بونيه: الذكاء الاصطناعي، واقعه ومستقبله، 1945، ترجمة د. على صبري فرغي، مجلة عالم المعرفة، العدد رقم 172، 1993م.

7- أمال عبد الرحيم عثمان: النموذج القانوني للجريمة، مجلة العلوم القانونية والاقتصادية، العدد 1، السنة 14، 1972م.

8- حدة أبو خالفة: النظام القانوني لمتعهد الإيواء عبر الإنترنت في القانون الجزائري والأردني، دراسات، علوم الشريعة والقانون، المجلد 45، العدد 4، ملحق ٢، ٢٠١٨م.
9- طارق الخن: الجرائم المعلوماتية، منشورات الجامعة الافتراضية السورية، 2018م.
10- محمد عرسان أبو الهيجا وعلاء الدين فواز الخصاونة، المسؤولية التقصيرية لمزودي خدمات الإنترنت عن المحتوى غير المشروع، مجلة الشريعة والقانون، جامعة الإمارات العربية المتحدة، مدينة العين، دولة الإمارات العربية المتحدة، العدد الثاني والأربعون، إبريل ٢٠١٠م.
11- محمد عرفان الخطيب: المركز القانوني للإنسآلة ((Robots، الشخصية والمسؤولية، دراسة تأصيلية مقارنة، قراءة في القواعد الأوروبية للقانون المدني للإنسآلة لعام 2017م، مجلة كلية القانون الكويتية العالمية، السنة 6، العدد 4، العدد التسلسلي 24، ربيع الأول/ربيع الثاني 1440هـ، ديسمبر 2018م.
12- محمود سلامة عبد المنعم الشريف: المسؤولية الجنائية للإنسآلة: دراسة تأصيلية مقارنة، المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي، مجلد 3 عدد 1 (2021م)، على الرابط التالي:
https://journals.nauss.edu.sa/index.php/AJFSFM/article/view/1122
13- وديع فرج: الأعمال التحضيرية والبدء في التنفيذ، مجلة القانون والاقتصاد، كلية الحقوق، جامعة القاهرة، العدد1، س 4.

خامساً: المراجع الأجنبية

1- Ch. VERDURE: Les hébergeurs de sites web: victimes ou régulateurs de la société de l'information,DCCR,nr68-2005, p. 38.

2- Chesney, R., and Citron, D. Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. Foreign Affairs, 2019.

3- Cholet Sylvie: La responsabilité du fournisseur d'hébergement, Paries, février 2001

4- Schuhl Christiane ; Cyber droit, le droit à l'épreuve de L'internet, 3 éd., Dunod, paris, 2002.

5- A. PILETTE: La directive, commerce électronique: un bref commentaire, A & M., 2001.

6- David L. Anderson ،Robert T. Arrigo ،Andy Schmidgall; Artificial Intelligence: Can a Machine Think? National Science Foundation Grants ،2006 ، p.1.

7- Edvinas Meskys, Julija Kalpokiene, Paulius Jurcys, Aidas Liaudanskas; Regulating Deep Fakes: Legal and Ethical Considerationsm Journal of Intellectual Property Law & Practice, Volume 15, Issue 1, January 2020.

8- Flynn (A.) & Henry (N.), Image-Based Sexual Abuse: An Australian Reflection, Women & Criminal Justice, 2019.

9- Franks (M.-A.), The Crime of "Revenge Porn", In: Alexander (L.), Ferzan (K.-K.) (eds.), The Palgrave Handbook of Applied Ethics and the Criminal Law, Palgrave Macmillan, 2019.

10-Hall (M.) and Hearn (J.), «Revenge pornography: gender, sexuality and motivations», Routledge, 2018

11-Martinez (C.), An argument for states to outlaw „revenge porn" and for congress to amend 47 U.S.C. §230: how our current laws do little to protect victims, Pittsburgh Journal of Technology Law & Policy, vol. 14 (2), 2014.

12-Hogan Lovells, Penelope Thornton, Patrick Fromlowitz, Aissatou Sylla, Rachel Shelbourne Fleeson and Margaret (Maggie) Kathryn Pennisi. Deepfakes: An EU and U.S. perspective, July 24 2020,

13-Kaplan, Andreas and Haenlein, Michael. (January–February 2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence, Kelley School

of Business, Indiana University. Elsevier Inc. Vol.62, I.1.

14-Rich, Elaine and Knight, Kevin. Artificial Intelligence, McGraw Hill companies Inc. 2006.

15-Russell, Stuart and Norvig, Peter. Artificial Intelligence: A Modern Approach Prentice Hall, 2002.

16-Lemouland, Les critères jurisprudentiels de l'infraction politique, R.S.C. 1988.

17-M. Caldwell, J. T. A. Andrews, T. Tanay, L. D. Griffin. AI-enabled future crime. Crime Science, 2020.

18-Matthew Ferraro. Texas Law Could Signal More State, Federal Deepfake Bans, Reprinted with Permission from Law360

19-Nguyen, Thanh & Nguyen, Cuong M. & Nguyen, Tien & Duc, Thanh & Nahavandi, Saeid. Deep Learning for Deepfakes Creation and Detection: A Survey.2019

20-Sales (J.) & Magaldi (J.), "Deconstructing the Statutory Landscape of "Revenge Porn": An Evaluation of the Elements That Make an Effective Nonconsensual Pornography Statute", American Criminal Law Review, Vol. 57(4), 2020.

21-V. J. Pinatel, "L'élément matériel de l'infraction devant la criminologie et les sciences de l'homme ", R. S. C. 1967.