د. محمـــود زكـــي زيـــدان
مدرس القانـــون الجنائـي –كلية الحقوق – جامعة طنطا

المواجهة الجنائية للاستخدام غير المشروع لتقنية التزييف العميق

(دراســـة مقارنـــة)

المراسلة: د. محمـــود زكـــي زيـــدان
مدرس القانـــون الجنائـي –كلية الحقوق – جامعة طنطا

معرف الوثيقة الرقمي (DOI): https://doi.org/10.54873/jolets.v4i1.170

البريد الإلكتروني: mzidan11194@gmail.com

نسق توثيق البحث:
محمـــود زكـــي زيـــدان، المواجهة الجنائية للاستخدام غير المشروع لتقنية التزييـــف العميـــق (دراســـة مقارنـــة)، المجلد الرابع، العدد الأول، إبريل ٢٠٢٤
صفحات ٢٠٣– ٣٢٢

الملخص:

ممـا لا شك فيه؛ أن جرائـم الذكاء الاصطناعي بوصفها جرائـم مستحدثة تتطور بسرعـة؛ لذلك يجب أن يواكب القانون الجنائي هـذا التطور في هذه الجرائم، ويعالج القصـور في نصوصـه لمواجهتها، حفاظًا على الحقوق المشروعـة التي يصيبها الضرر الكبـير من جراء تلك الجرائـم، ومن ثم يجب إقرار نظم قانونيـة جديدة إلا أنه يجب الحـذر من كـون هذه النظم غير مفيـدة، فتلك القوانين غير المفيـدة تضعف القوانين الضرورية.

إزاء هـذا التطـور التكنولوجي الهائل والكـم الكبير من المعلومات التـى أطلق عليها BIG DATA ظهـرت تقنيـة تسمى «التزييف العميق» واستخدمـت لأغراض عدة، منها على سبيـل المثال: التشهير والانتقام، والطامة الكـبرى أن تلك التقنيات صارت متاحة وميسـرة بشـكل كبـير ولا يحتاج تفعيلها أو التعامـل معها إلى أي مقابل مـادي أو تكلفة لاستخدامهـا وكل مـا تحتاجه هو بعض الدراية البسيطـة بالتكنولوجيا، فضلاً عن أنها ذات طابـع دولي، وذات دقة كبيرة فنجد العـالم فرانكلين فوير (Franklin Foer) في أوائـل ٢٠١٨ يقـول: «سنعيش قريبًا في عالم تخدعنا فيـه أعيننا» وذلك دليل على دقة هذه التقنية.

١- الكلمـات الافتتاحيـة: الـذكاء الاصطناعـي- الجرائـم المستحدثـة- البيانات الشخصية- التزييف العميق- التطور التكنولوجي.

Abstract

There is no doubt that artificial intelligence crimes as new crimes are developing rapidly, so the criminal law must keep pace with this development in these crimes, and address the shortcomings in its texts to confront them, in order to preserve the legitimate rights that suffer great damage as a result of these crimes, and then new legal systems must be approved, but it must be careful that these systems are not useful, as these useless laws weaken the necessary laws.

In the face of this tremendous technological development and the large amount of information and called BIG DATA, a technique called deepfakes appeared and was used for several purposes, for example: defamation and revenge, and the great catastrophe that these technologies have become available and facilitators greatly and do not need to be activated or dealt with to any material return or cost to use them and all you need is some simple knowledge of technology as well as it is of an international nature, and with great accuracy, so we find the world Franklin Foer (Franklin Foer) In early 2018, he says, «We will soon live in a world where our eyes deceive us,» a testament to the accuracy of the technology.

Keywords: Artificial Intelligence - New Crimes - Personal Data - Deepfakes Technological Development.

المقدمة:

يُصاحب التقدم العلمي ظهور أنماط جديدة من الجرائم، فقد ترتب على ثورة المعلومات والاتصالات[١]، والتي سميت بالثورة الصناعية الرابعة[٢] التي يعيشها العالم في الوقت الراهن ظهور أنماط جديدة من السلوك، تشكل جرائم جديدة[٣]؛ حيث أسهمت في تحويل الحياة المجتمعية عن كل ما هو تقليدي[٤]، فعجزت معظم النصوص القانونية السارية عن مد مظلتها لتوفير الحماية الجنائية ضد هذه الأفعال، وهو ما حدا بالمشرع في أغلب الدول إلى التدخل، وسن التشريعات الجنائية الجديدة، لتحكم هذه الأفعال في ثوبها الجديد، على نحو يساير به التقدم التقني الذي أحدثه الكمبيوتر وشبكة الإنترنت، ومع ذلك ما زالت أغلب التشريعات المعاصرة قاصرة عن الإحاطة بهذه الأفعال؛ إذ ما تزال الجريمة المعلوماتية تسبق التشريعات التي تحكمها بشكل كبير[٥].

ففي الماضي، كنا نعيش في عالم فقير المعلومات. لكن الآن ومع توافر المعلومات (البحث على الويب، ويكيبيديا، والخرائط الرقمية، وما إلى ذلك)، أصبحنا نواجه طوفانًا من البيانات، ونواجه بالكثير من المعلومات التي لا يمكننا تقييمها ومعالجتها. لقد أصبحنا -نحن بني البشر- مصابين بالعمى بسبب الكثير من المعلومات، وهذا

(١) ظهرت الثورة الصناعية الأولى عام ١٧٨٠ باختراع المحركات البخارية، ثم جاءت الثورة الصناعية الثانية ١٨٨٠ وهو اختراع الكهرباء، وظهرت الثورة الثالثة عام ١٩٧٠ بظهور الحاسب الآلي وعصر البرمجيات ثم أخيرًا الثورة الصناعية الرابعة في ٢٠١٦ وهي الثورة الرقمية الذكية. (د. محمد عرفان الخطيب: الذكاء الاصطناعي والقانون « نحو مشروع قانون مؤطر للذكاء الاصطناعي»، المجلة القانونية والقضائية، وزارة العدل القطرية، ع٢، ٢٠٢٠، ص٢٠).

(٢) أطلقت تسمية الثورة الصناعية الرابعة خلال المنتدى الاقتصادي في دافوس (سويسرا) في ٢٠١٦ (د. كلاوس شواب: الثورة الصناعية الرابعة-ملخصات لكتب عالمية تصدر عن مؤسسة محمد بن زايد، ٢٠١٧، ص٢)، وتعرف الثورة الصناعية بأنها اندماج العوالم الرقمية بالعوالم المادية، فجعلت تكنولوجيا العالم الافتراضي كأنه حقيقي. (د. سعاد شاهين: تكنولوجيا الفئات الخاصة في الثورات الصناعية، مجلة الجمعية المصرية للكمبيوتر التعليمي، المجلد العاشر، ع٢، ديسمبر ٢٠٢٢، ص٢١٨).

(٣) د. أحمد سعد على البرعي: تطبيقات الذكاء الاصطناعي والروبوت من منظور الفقه الإسلامي، مجلة دار الإفتاء المصرية، مجلد١٤، ع٤٨، يناير ٢٠٢٢، ص١٧.

(٤) أ.صابر الهدام: القانون في مواجهة الذكاء الاصطناعي، رسالة ماجستير، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة سيدي محمد بن عبد الله، ٢٠٢٢، ص١.

(٥) د. حاتم عبد الرحمن: الإجرام المعلوماتي، دار النهضة العربية، القاهرة، ٢٠٠٢، ص ٥.

يجعلنا عرضة للتلاعب. ولذا يثار التساؤل من ذا الذي يجب أن ينتج هذه المعلومات؟ هل هي الشركات، أم هي الدول؟ في عالم يتميز بالحمل الزائد للمعلومات التي أصبحت وقود هذا العصر[١]؛ حيث أمست المعلومات الموثوقة غير المتحيزة أكثر أهمية من أي وقت مضى ولذلك فإنه لكي ينجح المجتمع الرقمي[٢]، فيجب علينا اتخاذ تدابير وقائية ضد تلوث المعلومات[٣].

أعلنت منظمة الصحة العالمية في ٢ فبراير ٢٠٢٠، أنه إلى جانب جائحة COVID-19، نواجه: «وفرة من المعلومات الإعلامية – بعضها دقيق وبعضها غير دقيق – يجعل من الصعب على الناس العثور على مصادر جديرة بالثقة وإرشادات موثوقة عندما يحتاجون إليها»[٤]، وفي ضوء ذلك نجد أن فهم فئات المعلومات من الأمور بالغة الأهمية للوقوف والتواصل حول المشهد المعني، ومما يؤكد ذلك أن scholars قد شرحت العديد من التصنيفات المختلفة للمعلومات[٥]، أهمها:

المعلومات المضللة والتي لا تتسبب في ضرر: وهي المعلومات الخاطئة التي لا يتم إنشاؤها أو نشرها بقصد التسبب في ضرر من ذلك على سبيل المثال: المشاركة بحسن نية في علاجات COVID-19 الكاذبة.

المعلومات الخاطئة الشخصية: وهي المعلومات الحقيقية التي يتم استخدامها مع الرغبة في إلحاق الأذى بصاحبها من ذلك على سبيل المثال: نشر صور حميمية محرجة.

---

(١) د. محمد حسن عبد الله علي: النظام القانوني لحماية البيانات المعالجة إلكترونياً، دراسة تحليلية مقارنة في ضوء اللائحة الأوروبية وبعض التشريعات ذات العلاقة، مجلة العلوم القانونية، جامعة عجمان، الإمارات، ع١٤، يوليو٢٠٢١، ص٧٥.

(٢) وسميت الرقمية بأنها عملية الحصول على مجموعة من النصوص التقليدية وتحويلها إلى صور إلكترونية يمكن الاطلاع عليها من خلال تطبيقات الحاسب الآلي».

د. جيهان صبري محمد عبد الغفار: الحكم الشرعي للمخدرات الرقمية، مجلة كلية الشريعة والقانون، جامعة الأزهر، فرع أسيوط، ع٣٤، يوليو ٢٠٢٢، ج٢، ص١٩٥٤.

(3) Dirk Helbing: Towards Digital Enlightenment Essays on the Dark and Light Sides of the Digital Revolution, Springer Nature, 2019, p66
https://link.springer.com/content/pdf/10.1007/978-3-319-90869-4.pdf

(4) World Health Org. [WHO], Novel Coronavirus 2019-nCov Situation Report - 13 (Feb. 2, 2020), https://www.who.int/docs/default-source/coronaviruse/situation-re ports/20200202-sitrep-13-ncov-v3.pdf [https://perma.cc/A9HB-2BXJ].

(5) YAMAOKA-ENKERLIN: Anna. Disrupting disinformation: Deepfakes and the Law. NYUJ Legis. & Pub. Pol'y, 2019, p725.

المعلومـات المضللة بقصد الإضرار العـام: وهي المعلومات الكاذبة التي يتم إنشاؤها بقصـد الإضـرار العام أو تغيير التصورات عن الواقـع والحقيقة. ومن ذلك على سبيل المثال: مؤامرة «Piz-zagate» [١] التي انتشرت على نطاق واسع قبل الانتخابات الرئاسية الأمريكية لعام ٢٠١٦ [٢].

ومـن الجدير بالذكـر أن الثورات التكنولوجية تميل إلى خلـق مواقف غالبًا ما تؤدي إلى تخفيـف القيم الأخلاقية الفرديـة؛ حيث تمر الأسس والقيـم الثقافية والسياسية والاجتماعيـة في جميع أنحاء العالم بتغير صامـت، ولكنه هائل في ظل ظهور منتجات الحاسوب الجديدة، وتطور الثورة التكنولوجية بسرعة هائلة للدرجة التي أصبحت معها تجردنا من قدرتنا على التأقلم، وعلى الرغم من ذلك فإننا نحتاج باستمرار إلى مبادئ وقيـم أخلاقية جديـدة للتعايش مع المشهد المتغير؛ فلا يمكننـا صياغة ومناقشة ووضع مثل هذه المبادئ والقيم بسرعة كافية قبل أن تصبح قديمة. والأهم من ذلك، فإنه حتى لو تمكنا من التوصل إلى قيم ومبادئ أخلاقية جديدة، فسنظل نفتقر إلى النماذج التي يمكن من خلالها تطبيق هذه القيم والمبادئ[٣].

ويكفينـا فـي هـذا الصـدد أن نقـول إن الـذكاء الاصطناعي يأخذ خيـارات يمكن اعتبارهـا ذات طابع أو نتيجة أخلاقية إذا تم تنفيذها بواسطة الإنسان. فالحياة مليئة بالخيـارات الأخلاقية، غالبًا ما ينص القانون على إجابـات خاصة بهذه الخيارات[٤].

---

(١) نظرية المؤامرة Pizzagate هي مؤامرة تم تداولها على نطاق واسع خلال الانتخابات الرئاسية الأمريكية لعام ٢٠١٦، وتم فضح زيفها لاحقًا. حيث أكدت العديد من الوكالات عدم موثوقيتها، بما في ذلك قسم شرطة العاصمة في مقاطعة كولومبيا. حيث تم استهداف حساب البريد الإلكتروني الشخصي لمدير حملة هيلاري كلينتون جون بوديستا بهجوم تصيد احتيالي في مارس ٢٠١٦. وقـد تم نشـر رسائل البريد الإلكتروني الخاصة به من قبل ويكيليكـس في نوفمبر ٢٠١٦. فزعم أنصار نظرية مؤامرة Pizzagate أن رسائـل البريـد الإلكـتروني تحتوي على رسائل مشفرة تربـط العديد من المطاعم الأمريكيـة بكبار المسؤولين الديمقراطيـين المتورطين في الاتجار بالبشر وتجارة الجنس مع الأطفال، فقـام أعضاء من اليمين، والصحفيين المحافظين، وغيرهم بالمطالبة بمقاضاة كلينتون، وقاموا بنشر نظرية المؤامرة على وسائل التواصل الاجتماعي.
https://ar.wikipedia.org/wiki/%D9%86%D8%B8%D8%B1%D9%8A%D8%A9_%D9%85%D8%A4%D8%A7%D9%85%D8%B1%D8%A9_%D8%A8%D9%8A%D8%AA%D8%B2%D8%A7%D8%BA%D9%8A%D8%AA

(2) Claire Wardle & Hossein Derakhshan, Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking 20, Council of Europe DGI(2017)09 (Sept. 27, 2017), https://rm.coe.int/information-disorder-report-novem ber-2017/1680764666.

(3) Joseph Migga Kizza: Ethical and Social Issues in the Information Age, Sixth Edition, Springer International Publishing AG, 2017p53

(٤) جبريل العريشي: استخدام البيانات الضخمة والذكاء الاصطناعي في مواجهه جائحة فيروس كورونا المستجد، المجلة العربية للدراسات الأمنية، العدد ٣٦ع، ٢٠٢٠، ص٢٥١.

فالقتل الرحيم -على سبيل المثال- يعد غير قانوني في معظم البلدان، ويعنى القتل الرحيم Euthanasia (الانتحار بمساعدة) [١]، ومع ذلك يسمح به في هولندا وبلجيكا وكندا وسويسرا في ظل ظروف خاصة، تخضع لرقابة صارمة[٢].

وإزاء هذا التطور التكنولوجي[٣] الهائل، والكم الكبير من المعلومات، أو ما يطلق عليها[٤] BIG DATA ظهرت تقنية تسمي بالتزييف العميق، واستخدمت لأغراض عدة منها على سبيل المثال: التشهير والانتقام[٥]، والطامة الكبرى أن تلك التقنيات صارت متاحة وميسرة بشكل كبير ولا يحتاج تفعيلها أو التعامل معها إلى أي مقابل مادي أو تكلفة لاستخدامها وكل ما تحتاجه هو بعض الدراية البسيطة بالتكنولوجيا [٦] فضلاً عن أنها أصبحت ذات طابع دولي، وذات دقة كبيرة مما دفع العالم الكبير فرانكلين فوير (Franklin Foer) في أوائل ٢٠١٨ إلى القول: «سنعيش قريبًا في عالم تخدعنا فيه أعيننا» وهذا دليل على دقة هذه التقنية[٧].

---

(١) إنهاء حياة مريض ميؤوس من شفائه طبيًا بفعل إيجابي أو سلبي للحد من آلامه المبرحة، أو غير المحتملة، بناءً على طلبه الصريح أو الضمني، أو طلب من ينوب عنه، سواء عن طريق الطبيب أو شخص آخر، د.هدي حامد قشقوش: القتل بدافع الشفقة، دراسة مقارنة، دار النهضة العربية، ٢٠٠٦، ص٦.

(٢) د.منصور عمر المعايضة: المسؤولية المدنية والجنائية في الأخطاء الطبية، مركز الدراسات والبحوث، الرياض، ٢٠٠٤، ص٩٨، أ.مروة فرج: القتل الرحيم بين الشريعة والقانون الوضعي، رسالة ماستر، جامعة الشهيد حمه لخضر، ٢٠١٨، ص٤٠، د. السعدني على شويته: القتل بدافع الشفقة، رسالة دكتوراه، كلية الحقوق، جامعة طنطا، ٢٠١٠، ص١٤٥.

(٣) التطور هو نوع من التغير يأخذ صورة النمو من شكل بسيط إلى شكل معقد، د. عبد العزيز لطفي جاد الله: الجريمة السيبرانية وحماية أمن المعلومات، مؤسسة المروة للنشر والتوزيع، ٢٠٢٢، ص ٨٥.

والتكنولوجيا تعني كافة الأساليب الفنية التي يستخدمها الإنسان لإشباع حاجاته المختلفة وتحسين جودة حياته.

د. نائلة عادل قورة: جرائم الحاسب الآلي الاقتصادية دراسة نظرية وتطبيقية، منشورات الحاتي الحقوقية، ٢٠٠٥، ص٥٠.

(4) Amit Kumar; CHAHAL, Poonam. Artificial intelligence and machine learning algorithms. In: Research Anthology on Machine Learning Techniques, Methods, and Applications. IGI Global, 2022. p. 421

Rajiv Pandey, Sunil Kumar Khatri, Neeraj Kumar Singh, Parul Verma: Artificial intelligence and machine learning for EDGE computing. Academic Press, 2022.p xix.

(٥) د. مصطفى صلاح عبد الحميد: التزييف الرقمي وأثره على حجية الأدلة الرقمية في الدعاوى الجنائية، دراسة فقهية مقارنة، مجلة الشريعة والقانون، القاهرة، جامعه الأزهر، ع٤٠، أكتوبر ٢٠٢٢، ص٨٤٢ .

(٦) أ. جوارحي عبد الستار: جرائم الحاسوب-دراسة مقارنة بين الشريعة الإسلامية والقانون الجزائري، كلية العلوم الاجتماعية والإنسانية جامعة الشهيد حمة لخضر رسالة ماجستير، ٢٠١٥، ص ج.

د. محمد أحمد سلامة مشعل: الذكاء الاصطناعي وآثاره على حرية التعبير في مواقع التواصل الاجتماعي، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، مج١١، ع٧٧، سبتمبر ٢٠٢١، ص٥٠٥.

(7) Franklin Foer: The Era of Fake Video Begins The digital manipulation of video may make the current era of «fake news» seem quaint. May 2018
https://www.theatlantic.com/magazine/archive/2018/05/realitys-end/556877/

ومما لا شك فيه أن جرائم الذكاء الاصطناعي بوصفها جرائم مستحدثة تتطور بسرعة[١]، يجب أن يتواكب معها القانون الجنائي، وأن يعالج القصور في نصوصه لمواجهتها، حفاظًا على الحقوق المشروعة التي يصيبها الضرر الكبير من جراء تلك الجرائم[٢]، ومن ثم يجب إقرار نظم قانونية جديدة إلا أنه يجب الحذر من كون هذه النظم غير مفيدة، فتلك القوانين غير المفيدة تضعف القوانين الضرورية[٣].

إن الذكاء الاصطناعي يختلف نوعيًّا عن التقنيات الموجودة الأخرى؛ لأنه يتخذ أحيانًا قرارات مستقلة[٤]، وهذا يمثل تحديًا للأنظمة القانونية المعمول بها؛ لأننا أصبحنا – ولأول مرة – أمام تكنولوجيا ينسب اليها – بعيدًا عن الإنسان– كُلٌّ من السلوك الإجرامي والنتيجة الإجرامية معًا، ومن ثَمَّ يلزم وضع أطر قانونية لتفادي الآثار السلبية لتطبيقات الذكاء الاصطناعي[٥].

إشكالية البحث: يثير هذا البحث العديد من التساؤلات المهمة، ويحاول الإجابة عليها، منها:

ماهية تقنية التزييف العميق؟

- هل هناك فرق بين تقنية التزييف العميق وغيره من برامج تركيب الفيديوهات (الفوتوشوب نموذجًا)؟
- ما خصائص تقنية التزييف العميق؟ وهل هناك إيجابيات ناشئة عن استخدامها؟
- وما ماهية الأفعال التي تمثل جريمة عند استخدامها بشكل خاطئ، وعلى من تقع المسئولية الجنائية عن استخدام تلك التقنية؟

---

(١) د.عبد الفتاح بيومي حجازي: الجريمة في عصر العولمة، دار الفكر الجامعي، الإسكندرية، ٢٠٠٧، ص ٦٣.

د.وليد سعد الدين محمد سعيد: المسئولية الجنائية الناشئة عن تطبيقات الذكاء الاصطناعي، مجلة العلوم الاقتصادية والقانونية، ع٢، يوليو٢٠٢٢، ص ٤٨٨.

(2) Jean-Nicolas ROBIN: La matière pénale à l'épreuve du numérique, THÈSE PRÉSENTÉE POUR OBTENIR LE GRADE DE DOCTEUR, UNIVERSITÉ DE RENNES, 2017, p.27

(٣) د.محمد محمد عبد اللطيف: المسئولية عن الذكاء الاصطناعي بين القانون الخاص والعام، بحث مقدم إلى مؤتمر الجوانب القانونية والاقتصادية للذكاء الاصطناعي وتكنولوجيا المعلومات، كلية الحقوق –جامعة المنصورة، ٢٣–٢٤ مايو ٢٠٢١، ص٤.

(٤) د. منى محمد العتريس: جرائم تقنيات الذكاء الاصطناعي والشخصية القانونية الإلكترونية المستقلة، دراسة مقارنة، مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، ع ٨١، سبتمبر ٢٠٢٢، ص١١٥٢.

(٥) د. وليد سعد الدين محمد سعيد: مرجع سابق، ص٤٩٩.

أهمية البحث:

أصبحت الفيديوهات المزيفة ذات أضرار اجتماعية وسياسية، فلقد شَهدت السنوات الأخيرة انتشارًا هائلاً للفيديوهات المزيفة، فلقد ارتفع ٩٠٠٪ بين عامي ٢٠١٩-٢٠٢٠، لذا كان لابد من التعرض لمخاطر التزييف العميق، ومعرفة الجرائم المكونة للاستخدام غير المشروع لتلك التقنية الخطرة.

صعوبات البحث:

لعلَّ حداثة تقنية التزييف العميق؛ لكونها تعتمد على الذكاء الاصطناعي، وعدم وجود آلية لمواجهته، وعدم النص عليها في نصوص القانون المصري وفي التشريعات المقارنة هو ما يمثل صعوبة كبيرة على كل باحث يرتاد هذا المجال.

منهج البحث:

تتطلب دراسة المواجهة الجنائية للاستخدام غير المشروع لتقنية التزييف العميق الرجوع إلى النصوص المختلفة، وفي التشريعات المقارنة، لذلك جاء البحث معتمدًا على المناهج التالية:

١- المنهج التحليلي: حيث يتناول البحث النصوص القانونية بالتحليل، ويحاول إيجاد حلول لمنع ارتكاب أي جرم.

٢- المنهج المقارن: حيث يرنو البحث إلى المقارنة بين النصوص القانونية المختلفة، وفي ضوء ذلك تكون هذه الدراسة (تحليلية مقارنة).

خطة البحث:

يمكن تقسيم البحث بالصورة التي تخدم إشكاليته الرئيسية في أربعة فصول:

- **الفصل الأول: ماهية تقنية التزييف العميق.**
- **الفصل الثاني: التكييف الشرعي والقانوني لتقنية التزييف العميق.**
- **الفصل الثالث: الصور التجريمية الناشئة عن الاستخدام غير المشروع لتقنية التزييف العميق.**
- **الفصل الرابع: المسئولية الجنائية عن الاستخدام غير المشروع لتقنية التزييف العميق.**

الفصل الأول

ماهية تقنية التَّزييف العميق

تمهيد وتقسيم:

مـع بدايات القرن الحـالي كان برنامج الفوتوشـوب Adobe Photoshop (وهو من أهـم التطبيقـات المعروفـة[١] بتركيب الصور) يعد واحـدًا من أشهـر وأخطر البرامج المستخدمـة لقصّ ودمج الصـور[٢]، وكان الشخصـ العادي لديه المقـدرة على تمييز تلـك الصـور المفبركة[٣]. إلا أنه مع التطـور الهائل للتكنولوجيـا وللمعلومات ظهرت ما يعـرف بتقنيـة (Deep fakes)؛ ممَّا شكل صعوبة في التفرقـة بين ما هو مزيف وما هو حقيقـي[٤]، فممَّـا لا شكَّ فيه أن هـذه التقنية تُعد أخطر بكثير مـن غيرها؛ ولذا يُعنى هـذا الفصل بتوضيح مفهوم هـذه التقنية، وتمييزها عن التَّزييـف السطحي، ثمَّ بيان خصائصها، وذلك في ثلاثة مباحث، وذلك على النحو التالي:

- **المبحث الأول: مفهوم تقنية التَّزييف العميق.**
- **المبحث الثاني: التمييز بين التَّزييف السطحي والتزييف العميق.**
- **المبحث الثالث: خصائص تقنية التَّزييف العميق.**

---

(١) د. عبد الله السعود السراني: مهارات التحقيق في جرائم تزييف العملة، جامعة نايف العربية للعلوم الأمنية، ٢٠١٠، ص٥٥.

(٢) د. شيريـن كـدواني، د. شريهـان توفيق: الإعلام الرقمي تشريعـات وأخلاقيات النشر، العربية للنشـر والتوزيع، بدون تاريخ نشر، ص١٥.

(٣) د. شيلا براون، ترجمة أ. هدى فؤاد: الجريمة والقانون في ثقافة الإعلام، مجموعة النيل العربية، ٢٠٠٦، ص١١٤.

(4) Dava mckay: How Deepfakes Are Powering a New Type of Cyber Crime
https://www.howtogeek.com/devops/how-deepfakes-are-powering-a-new-type-of-cyber-crime/

المبحث الأول
مفهوم تقنية التَّزييف العميق

التَّزييف لغةً:

التَّزييف مصدر من الفعل زيف ويعني غش الشيء وتغييره، غش النقود وتزويرها، فزاف الدراهم أي صارت مغشوشة، وقيل إنَّ الدرهم زيف وزائف[١]، فالزيف هو الرديء فيقال في حديث ابن مسعود: أنه باع نفاية بيت المال وكان بيعًا زيوفًا؛ أي رديئا والزائف غير الصالح للتعامل به[٢].

التَّزييف اصطلاحًا:

لقد تعرض القرآن الكريم لمصطلح التَّزييف؛ ﴿وَإِذَا لَقُوا الَّذِينَ آَمَنُوا قَالُوا آَمَنَّا وَإِذَا خَلَا بَعْضُهُمْ إِلَى بَعْضٍ قَالُوا أَتُحَدِّثُونَهُمْ بِمَا فَتَحَ اللَّهُ عَلَيْكُمْ لِيُحَاجُّوكُمْ بِهِ عِنْدَ رَبِّكُمْ أَفَلَا تَعْقِلُونَ﴾[٣]، ومن الواضح من الآية الكريمة أن التَّزييف في القرآن الكريم يأتي بمعنى التحريف والتغيير.

ولقد عرف بعض الفقهاء التَّزييف بأنه: «عملية مادية لإعادة إنتاج عمل بطريقة غير مشروعة وغير صحيحة، للكذب والخداع لأجل إلحاق الضرر بأحد الأفراد»[٤].

وعرفه البعض بأنه: «وصف الشيء بخلاف صفته، حتى يخيل إلى من سمعه أو رآه أنه بخلاف ما يوجد عليه، فهو جعل الباطل بصورة حق»[٥]، فهو إعادة إنتاج منتج أصلي بشكل مطابق للواقع والأصل[٦].

والتَّزييف في القانون مقترن بالعملة والمسكوكات؛ إذ تعرفه المادة (٢٠٢) من قانون العقوبات المصري على أنه «انتقاص شيء من معدن العملة أو طلائها بطلاء يجعلها

---

(١) محمد بن منظور: لسان العرب، ج٩، بيروت، ١٩٩٨، ص١٤٣.

(٢) المبارك بن محمد بن الأثير: النهاية في غريب الحديث والأثر، ج٢، دار الكتب العملية، بيروت، ١٩٧١، ص٢٩١.

(٣) البقرة: ٧٥.

(٤) د. عبد الفتاح حجازي: الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، ٢٠٠٢، ص٤٥.

(٥) الوزير أبي المظهر يحيى الشيباني: اختلاف الائمة العلماء، ج٢، دار الكتب العلمية، بدون سنة نشر، ص٤٢٥.

(6) Delphine Baize: De la contrefaçon à l'imitation, revue française de gestion, juin-juillet-aout 1999, p: 76-78.

شبيهًـا بعملة آخرى»، إلا أن هذا التعريف أصبـح ماضيًا مع حداثة وتقدم التكنولوجيا، فلقـد استخدم مصطلح التَّزييف في مجـال التكنولوجيا بمعنى الشـيء المزور، ويعمل علـى الخداع والتضليـل، كما استخدم في تطبيقات الـذكاء الاصطناعي، وتعتبر تقنية التَّزييف العميق من تطبيقات الذكاء الاصطناعي.

تعريف تقنية التَّزييف العميق:

لعـلَّ هـذا المصطلـح جديد علـى الآذان؛ حيث إنه معنـي بالمقاطع المرئيـة التي تتمّ معالجتهـا لتبـدو بشكل مخالـف لما هي عليه؛ كتعديـل الصوت أو الصـورة؛ لذا عرفت التقنيـة التي تعنى بذلك بأنها: «تقنية تستخدم الذكاء الاصطناعي(AI)[١] لوضع أحد الوجـوه علـى جسد شخص آخـر عبر استخـدام خوارزميـات Algorithms[٢] الذكاء الاصطناعي»[٣].

كما عرفت بأنها: «إحدى تطبيقات الذكاء الاصطناعي التي تعمل على تركيب محتوى الفيديوهـات بشكل دقيـق يحاكي الفيديو الأصلـي وإن كان يختلف عنـه في مضمونه ومحتـواه»[٤]، فعرفت بأنها عمليـة غير مستقلة تطبق خوارزميـات الذكاء الاصطناعي على الموضوع والإنتاج[٥].

وفي ضوء ذلك يمكن لنا تعريف التَّزييف العميق بأنه: «كل محتوى مرئي[٦] أو صوتي تمَّ التلاعب به بواسطة برامج متطورة، وتمَّ بموجبه تركيب صورة المستهدف على فيديو

(١) ولعل AI هي اختصار لكلمة Artificial Intelligence والتي تعني الذكاء الاصطناعي.

(٢) هـي أساس الـذكاء الاصطناعي وأهم ركن لديه وهـي تعني مجموعة من القواعـد الحسابية والخطـوات الرياضية المتتابعة والمتعاقبـة لإعطـاء نتيجـة معينـة، ويمكن أن تستخـدم في التحليـل والتصنيف، ولعل هـذا المصطلح مشتق مـن اسم العالم الرياضـي محمـد بن موسي الخوارزمي، د. محمود سلامة الشريف: الطبيعـة القانونية للتنبؤ بالجريمة، المجلة العربية لعلوم الأدلة الجنائية والطب الشرعي مجلد ٣، عدد٢، سنة ٢٠٢١، ص ٣٤٣.

د. أروى بنـت عبـد الرحمن بن عثمان الجلعود: أحكام تطبيقات الذكاء الاصطناعي فـي القضاء، الجمعية العلمية القضائية السعودية، ١٤٤٤هـ، ص٤٣.

(3) Michael Filimowicz: Deep Fakes Algorithms and Society, Routledge, 2022p1

(4) Floridi Luciano: Artificial Intelligence, Deepfakes and the Future of Ectypes, Philos. Technol31, 2018. P320

(5) Loveleen Gaur: DeepFakes Creation, Detection, and Impact, CRC Press, 2023,p3

(٦) هو كل محتوى متحرك مسجل على مادة إلكترونية لإعادة مشاهدتها أكثر من مرة يشمل الصور الثابتة والمقاطع المتحركة، راجع في ذلك د. عمار الحسيني: التصوير المرئي والتسجيل الصوتي وحجيتهما في الإثبات الجنائي، المركز العربي، ٢٠١٧، ص٢٥.

لجعله يقول ويفعل ما لم يحدث منه[١]، في سيناريوهات مختلفة؛ ومن ثمَّ نشر الفيديو المزيف، أو مقطع الصوت عبر شبكة الإنترنت لخداع الجمهور[٢].

وإذا نظرنا إلى البرلمان الأوروبي نجده يرى أن التزييف العميق ذو مدلول واسع عن التطبيقات الإلكترونية الأخرى، التي تقف عند حد تعديل البيانات الأصلية؛ حيث إنَّ التَّزييف العميق يهدف إلى توليد وتقليد صوت أو صورة أو مقاطع فيديو ليس لها علاقة بالواقع[٣].

وما من شك في أن هذه التقنية تحمل في طياتها العديد من الإيجابيات والسلبيات، ولعلَّ التساؤل المطروح في أذهاننا الآن هو عن ماهية الإيجابيات النابعة من مثل هذه التقنية؟

إنَّ تقنية التَّزييف العميق لها العديد من الإيجابيات في العديد من الصناعات؛ كالأفلام السينمائية والألعاب الترفيهية، من ذلك على سبيل المثال:

١- استخدام تقنية التَّزييف العميق في الأعمال السينمائية: حيث يمكن إنتاج مقاطع

(1) Maryam Taeb, Hongmei Chi: Comparison of Deepfake Detection Techniques through Deep Learning. J. Cybersecur. Priv. 2022,p 89–. https://doi.org/10.3390/jcp2010007& Claire Langlais-Fontaine: Démêler le vrai du faux: étude de la capacité du droit actuel à lutter contre les deepfakes, La Revue des droits de l'homme, N°18 | 2020, p.1.https://journals.openedition.org/revdh/9747 & GERSTNER, Candice R.; FARID, Hany: Detecting Real-Time Deep-Fake Videos Using Active Illumination. In: Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition. 2022. p. 53-60& Ashifur Rahman , Md. Mazharul Islam , Mohasina Jannat Moon1 , Tahera Tasnim , Nipo Siddique1 , Md. Shahiduzzaman *, and Samsuddin Ahmed: A Qualitative Survey on Deep Learning Based Deep fake Video Creation and Detection Method. Aust. J. Eng. Innov. Technol, 2022, p.13-26 https://www.researchgate.net/profile/Ashifur-Rahman/publication/358322160_A_Qualitative_Survey_on_Deep_Learning_Based_Deep_fake_Video_Creation_and_Detection_Method

(٢) د. ممدوح عبد المطلب: خوارزميات الذكاء الاصطناعي وإنفاذ القانون، دار النهضة العربية، ٢٠٢٠، ص٩.

د. معاذ الملا: الأبعاد التاريخية لتطوّر نظرية المسؤولية الجزائية وجدلية تطبيقها في عصر الذكاء الاصطناعي: دراسة تحليلية واستشرافية، ع١٠، الجزء الأول ملحق خاص، سبتمبر٢٠٢١، ص١٠٧.

Hin-Yan Liu,Andrew Mazibrade:Artificial Intelligence affordance: Deep Fakes as Exemplars of AI Challenges to Criminal Justice Systems,2020,United Nations Interregional Crime and Justice Research Institute ,2020,p59

(3) 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 ‹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'.
European Parliamentary Research Service Scientific: Tackling deepfakes in European policy- STUDY Panel for the Future of Science and Technology EPRS | Foresight Unit (STOA) PE 690.039 – July 2021,p XIIIhttps://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf
& Bo Zhao ,Shaozeng Zhang, Chunxue Xu, Yifan Sun&Chengbin Deng: Deep fake geography? When geospatial data encounter Artificial Intelligence. Cartography and Geographic Information Science, 2021, p. 338-352

الفيديـو الاصطناعيـة بتكلفة لا تزيد علـى عشرة بالمائة من التكلفـة العادية، وتعويض غياب الممثلين لظروف خاصة، فعلى سبيل المثال: يمكن إصدار أفلام من بطولة ممثلين ماتـوا منذ فترة طويلة؛كما حدث عنـد ظهور الممثل بول ووكر في فيلم فاست فوريس 7 بعـد أن مات بحادث سيارة بمدة طويلـة[١]، وأنتج فيلم من بطولة (روبرت دينيرو) هو فيلم THE Irish Man عن طريق تقنية التزييف العميق، ودُمج الممثل الراحل Cushing peter في فيلم A Star Wars story عام ٢٠١٨ رغم أنه توفى قبل ذلك التاريخ[٢].

٢- إنتـاج تسجيـلات صوتية تاريخية وإعادتهـا للواقع: من ذلك علـى سبيل المثال: خطـاب الرئيس الأمريكـي «جون كيندي»[٣] الذي كان قد أعـده ليلقيه على الأمريكيين قبل اغتياله؛ حيث تم استخدام تقنية التزييف العميق مما جعل الخطاب يتم إلقاؤه بعد وفاة المذكور بنحو خمسة وخمسين عامًا وكأنه هو بنفسه الذي يلقيه![٤].

٣- استخـدام تقنيـة التزييف العميق فـي التوعية الإيجابية: وذلـك بدبلجة صوتية بشتـى اللغـات؛ فها هو (ديفيد بيكهـام) في حملة التوعية بالملاريـا ٢٠١٩ ظهر وكأنه متعدد اللغات، وذلك نتيجة لاستخدام خوارزميات الذكاء الاصطناعي، وتقنية التَّزييف العميـق[٥]، ويوضح مثـال (بيكهام) حقيقة أن تقنيـة التَّزييف العميـق لديها إمكانات مفيـدة هائلـة في التطبيقـات التجارية. وممَّا لا شـكَّ فيه أنه سيسهـم في أن يصبح

---

(١) د. كريمـة غديـري: التزييـف العميـق، نشـأة التقنيـة وتأثيرهـا على مجلـة الرسالـة للدراسـات الإعلامية، المجلـد ٥، ع٤، ديسمبر٢٠٢١، ص١٢٨.

(٢) د.ولاء الناعـي: إدراك مستخدمـى مواقع التواصـل الاجتماعي لتهديدات التزييف العميق وعلاقتـه باستخدامهم الآمن لتلك المواقع، المجلة العلمية لبحوث الصحافة، كلية الإعلام، جامعة القاهرة، ع٢٤، ج٣، ٢٠٢٢، ص٣٩٦

(٣) هو سياسي أمريكي تولّى منصب الرئيس الخامس والثلاثين للولايات المتحدة من ٢٠ يناير ١٩٦١ حتى اغتياله في ٢٢ نوفمبر ١٩٦٣.
https://ar.wikipedia.org/wiki/%D8%AC%D9%88%D9%86_%D9%83%D9%8A%D9%86%D9%8A%D8%AF%D9%8A

(٤) وتمكـن المهندسـون مـن إعادة صياغة صوت كينيدي من خـلال تحليل تسجيلات لأكثر من ٨٠٠ خطـاب وتصريح إذاعي، ثم استخدموا بعد ذلك اللقطات الصوتية لإنشاء صوت الرئيس الأمريكي الـ ٣٥ وهو يلقي الخطاب. ويأتي هذا الخطاب الذي تم إنشاؤه رقميًّا، كجزء من مشروع صحيفة «تايمز أو لندن» وهو «JFK: Unsilenced».
John McCarthy : 'JFK' finally recites his last speech – 55 years after his death – thanks to AI https://www.thedrum.com/news/2018/03/16/jfk-finally-recites-his-last-speech-55-years-after-his-death-thanks-ai

(٥) د. كريمة غديري: مرجع سابق، ص١٢٨.
Thanks to technology developed by the company Synthesia AI, Beckham can be seen seamlessly speaking nine languages -- English, Spanish, Kinyarwanda, Arabic, French, Hindi, Mandarin, Kiswahili and Yoruba -- in the public appeal.
How we made David Beckham speak 9 languages https://www.synthesia.io/post/david-beckham

إنشاء محتوى الفيديو أرخص بكثير، وسيسهل بلا شكٍّ وجود موجة من نماذج الأعمال الجديدة، وسيسهم أيضًا في وجود أشكال جديدة من الاتصالات[١].

٤-التطبيقات الطبية: يمكن أن يكون للتزييف العميق من نوعية Sdf Deep استخدامات إيجابية كبيرة لأغراض تجارية واجتماعية، من ذلك على سبيل المثال: إنشاء صور طبية مقلدة لأغراض التدريب، ومن الجدير بالذكر أن (CereProc) هي شركة تستخدم تقنية مزيفة عميقة لإنشاء أصوات من أجل الأشخاص الذين يفقدون القدرة عن الكلام بسبب أورام الحنجرة عن طريق حركة الشفاة[٢].

٥- الاستخدامات التجارية للتزييف العميق Commercial Uses of Deep Fakes: إن تقنية التَّزييف العميق مفيدة اجتماعيًّا طالما يتمّ استخدامها لأغراض مشروعة. وفي شأن الاستخدامات التجارية[٣]، ينبغي أن تكون الأطراف قادرة على الاعتماد على القواعد القائمة بشأن الملكية الأوَّلية، أو مبدأ العمل المؤدى مقابل أجر[٤].

٦- مراكز وخدمات الاتصال: يمكن استخدام التزييف العميق لتكوين أصوات لتقديم خدمة الاستقبال في المؤسسات المختلفة مثل الفنادق والبنوك... وغيرها[٥].

٧- الأغراض الإبداعية: Creative Deep Fakes إنَّ تقنية التَّزييف العميق تفتح فرصًا لا حصر لها لاستخدام تلك التكنولوجيا لأغراض إبداعية وعلمية من قبل الطلاب أو الفنانين. فمن المؤكد أن شبكات GANs تمكن منشئ المحتوى من إنشاء محتوى جديد وتطوير أشكال جديدة من التعبير الإبداعي؛ حيث يمكن إنشاء مقاطع مزيفة عميقة كشكل من أشكال المحاكاة الساخرة أو السخرية (مقاطع الفيديو، الميمات، ... إلخ[٦]).

وبناءً على ما تقدم؛ يمكن النظر إلى التَّزييف العميق على أنه وسيلة تسهل التفاعلات الإبداعية والمناقشات السياسية، وتشكل جزءًا أساسيًّا من حرية التعبير، إلا أن واحدة من العواقب غير المقصودة لاستخدام تكنولوجيا التَّزييف العميق في البيئة الإبداعية

(1) Mike Butcher: 'The startup behind that deep-fake David Beckham video just raised $3', available at: https://techcrunch.com/2019/04/25/the-startup-behind-that-deep-fake-david-beckham-video-just-raise d-3m

(٢) دليل التزييف العميق: مرجع سابق، ص٤.

(3) Patil M., Rao M: Studying the Contribution of Machine Learning and Artificial Intelligence in the Interface Design of E-commerce Site. In: Satapathy S., Bhateja V., Das S. (eds) Smart Intelligent Computing and Applications. Smart Innovation, Systems and Technologies, vol 105. Springer Singapore, 2019, p. 197.

(4) Dr. Edvinas Meskys, Julija Kalpokiene, Aidas Liaudanskas Dr. Paulius Jurcys: Regulating Deep-Fakes: Legal and Ethical Considerations. P10

(٥) د. أحمد الخولي: مرجع سابق، ص٢٥٤٣.

(6) Dr. Edvinas Meskys, Julija Kalpokiene, Aidas Liaudanskas Dr. Paulius Jurcys: Regulating Deep-Fakes: Legal and Ethical Considerations. P10

أو التعليميــة هي أنها يمكن أن تؤدي إلى البلطجة بين الأطفال في المدارس، مثل التنمر الذي يحدث من بعض الأطفال على بعض.

وعلى الرغم من الإيجابيات النابعة عن استخدام تلك التقنية إلا أنها يشوبها العديد من السلبيات، ولعلَّ أهمها:

١-الاعتداء على الحسابات المصرفية:

لا يقتصــر انتحال الهوية المستند على الذكاء الاصطناعــي على الصور فقط؛ حيث إنه من الممكن أن يؤدي استخدام صوتيات مُتزامنة الحجم بهدف انتحال الهوية وإنشاء إشــارات صوتيــة هي إشــارات 1D والتي لها طبيعــة مختلفة جدًّا عــن الصور ومقاطع الفيديــو، وتحتاج إلى طــرق مختلفة ومتقدمــة لتطويرها لاستهداف عمليــات التزوير والتزييف باستخدام تقنية التَّزييف لصوت أحد الأشخاص ليقول ما لم يَقُله[١].

ففي سبتمبر ٢٠١٩، قام عدد من المجرمين بتزييف صوت الرئيس التنفيذي للشركة التــي يعْملــون بها، بما يجعله كأنه طالبهم فــي هذا المقطــع بتحويل مبلغ ٢٤٣ ألف دُولار لحســاب أحد الأشخاص وقــد كان[٢]، وليست هذه الواقعة هى الوحيدة في ذلك المجال إذ انــه في ينايــر ٢٠٢٠ تم التلاعب وإصدار صــوت لإحدى الشــركات الكبرى بإجراء مكالمــة هاتفية لمدير فرع أحــد البنوك الإماراتية طلب فيها تحويل مبلغ ٧٥٧ , ٩٩٨ , ١٩ دولارًا أمريكيًّــا وهــو ما تمَّ بالفعل إلا أنه تمَّ كشــف أكذوبة تلك المكالمة وكونها مزيفة[٣]، وأيضًــا الشركــة الألمانية التي تمَّ التحايل عليها بمبلغ٢٢٠ ألــف دولار بعدما تمَّ التلاعب واستخدام التَّزييف العميق لتقليد صوت أحد المديرين التنفيذيين بها[٤].

(1) Husrev Taha Sencar, Luisa Verdoliva, Nasir Memon: Multimedia Forensics, 2022, Springer, p326

(٢) انظر في ذلك المقالة المنشورة في صحيفة « the Well StreetJournal» حول تلك الجريمة Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case»Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime (Case - WSJ (www-wsj-com.translate.goog

(3) Martin Anderson: Deepfaked Voice Enabled $35 Million Bank Heist in 2020October 15, 2021 Deepfaked Voice Enabled $35 Million Bank Heist in 2020 - Unite.AI (www-unite-ai.translate.goog)

(٤) قنــاة العــين الإخباريــة رابــط :-https://al-ain.com/article/deefacke-the-future-of-smart-software laws

د. أحمــد مصطفى محرم: استخدامات الذكاء الاصطناعي –استخدام تقنية التزييف العميق في قذف الغير، مجلة البحوث الفقهية والاقتصادية، أكتوبر ٢٠٢٢، ص٢٥١٠.

٢- التلاعب وتغيير الأدلة الجنائية:

حيث إنَّ تقنية التَّزييف العميق تُتيح تكوين مقاطع فيديوهات عدة لأشخاص يظهرون بأنهم يقتلون أو يسرقون أو يرتكبون جرائم، ولذا حذرت الشرطة الأوروبية «يوروبول» من التَّوَسُّع في استخدام تقنية «التَّزييف العميق»، بل وجعلت مكافحة هذا الأمر أولوية لها(١).

ليس ذلك فحسب، فهذه التقنية مؤثرة في وسائل الإثبات، خاصة في أداء الشهادة بواسطة تقنية الاتصال عن بُعد(٢)؛ سواء عن طريق (الفيديو كونفرانس) والذي عرف بأنه: محادثة مسموعة ومرئية بين طرفين أو أكثر عبر وسائل الاتصال الحديثة لتحقيق الحضور عن بُعد(٣) وتُعد تقَنيّة (الفيديو كونفرانس) التّقَنيّة الأهم في حماية الشهود أمام القضاء، فتلك الخاصية تتضمن افتراضًا مجازيًّا لحضور الشهود والخبراء لقاعة الجلسة التي تتمّ فيها المحاكمة بصوتهم عبر سماعات، وصورتهم عبر شاشة عرض(٤)، حيث تسمح هذه التّقَنيّة باجتماع أكثر من شخصين، من أماكن مختلفة ومشاركة ورؤية أطراف آخرين، كما يمكن من خلالها توجيه الأسئلة والإجابة عليها(٥)، أو تقنية التيلي كونفرانس حيث تُعد هذه التّقَنيّة أحدث أساليب الاتصال الحديثة، وتعرف بأنها: «مؤتمرٌ صوتيٌّ يشارك فيه طرفان أو أكثر بواسطة وسائل الاتصالات السلكية واللاسلكية»(٦).

---

(1) https://arabic.euronews.com/2022/04/29/europol-warns-increasing-use-of-deep-fakes-crime-world
LANGLAIS-FONTAINE, Claire. Démêler le vrai du faux: étude de la capacité du droit actuel à lutter contre les deepfakes. La Revue des droits de l'homme. Revue du Centre de recherches et d'études sur les droits fondamentaux, 2020.

(٢) يُقصد بالوسائل التكنولوجية الحديثة لحماية الشهود أن يكون هناك حائلٌ بين الشهود وبين الجناة، بحيث يتمكن القاضي من الاستماع لكل منهما دون الكشف عن هوية الشهود.
راجع في ذلك مؤلفنا: الحماية الجنائية للشهود، دراسة مقارنة، رسالة دكتوراه، جامعة طنطا، ٢٠٢١، ص٤٨٥.

(٣) قانون الاتحاد لدولة الإمارات العربية المتحدة رقم ٥ لسنة ٢٠١٧ في المادة الأولى.

(٤) د. رامي متولي القاضي: توظيف تكنولوجيا المعلومات في مجال الإجراءات الجنائية، الفيديو كونفرانس نموذجًا، أعمال مؤتمر القانون والتكنولوجيا، الفترة من ٩ – ١١من ديسمبر ٢٠١٧، ج الأول، ص ١٠.
وتقنية الفيديو كونفرانس تستخدم بشكل مستمر في الحياة اليومية في الشركات والإدارات العامة، ويوجد نحو ٨٥٠٠٠ وحدة نظام مراقبة عن بُعد تم بيعها في أوروبا في سنة ١٩٩٧ وقد بيع منها في إيطاليا وحدها حوالي ٣١٠٠٠ عام ١٩٩٨.
Giuseppe tila: problemes techniques et de cout petites affiches n41 fevrier 1999 p 8.
CEDH. Cour 10 mai 2016 Affaire LUKACSFY C. ROUMANIE decision n 5659/7.

(٥) أ. حاتم فتحي البكري: مبدأ شفهية التقنيات الحديثة في المحاكمات الجنائية، مجلة البحوث القانونية، كلية الحقوق، جامعة المنصورة، ع ٤٩، إبريل ٢٠١١، ص ٧٥.

(٦) مؤلفنا: الحماية الجنائية للشهود، مرجع سابق، ص٤٩١.

ومـن ثمَّ فمـن الممكن استخدام تقنية التَّزييف العميق فـي تزييف الشهادة لشخص ما متقمصًا شخصيةً آخرى[١].

٣- الاستخدام غير المشروع للأغراض السياسية:

استخدمـت تلـك التقنيـة في الأغراض السياسية عـن طريق تزييـف مقاطع عبر استخدام تلك التقنيات لرجال السياسة للتشهير بهم، وهناك عدة أمثلة لذلك، أشهرها على سبيل المثال:

أ) أن الرئيس الأمريكي (دونالد ترامب) سخر في مايو ٢٠١٨ من القرارات السياسية لدولـة بلجيكا؛ حيث كان الحزب الديمقراطـي الاجتماعي في بلجيكا قد نشر على (Twitter وFacebook) فيديـو مدتـه دقيقة واحدة يظهر فيـه الرئيس (ترامب) وهـو يتحـدث باللغة الإنجليزية قائـلا: «أعزائي بلجيكا، هذه صفقـة ضخمة. كما نعلـم، كان علينا الانسحاب مـن اتفاقية باريس للمناخ، وعليكـم أنتم كذلك، نعلم جميعًـا أن تغير المناخ مزيف، مثل هذا الفيديـو[٢]»، إلا أن مشاهدات هذا الفيديو وصلت إلى عشرين ألف مشاهدة في يوم واحد، وكان عدد كبير من المشاهدين قد خدعوا بالفعل بهذا الفيديو؛ لأنهم اعتقدوا أنه كان مقطعًا أصليًّا لترامب[٣].

ب) انتشـار فيديوهات مزيفة عديـدة للرئيس الأمريكي (أوبامـا) يَسْخَر فيها من خليفته (دونالد ترامب) أثناء المنافسة بينهما في الانتخابات الرئاسية[٤].

ج) انتشار فيديو مزيف للرئيس الأوكراني (Zelenskyy)على مواقع التواصل الاجتماعي أثناء الحرب بين روسيا وأوكرانيا يُخْبِرُ جنوده بضرورة إلقاء الأسلحة والاستسلام[٥].

---

(١) د. أروى بنت عبد الرحمن: مرجع سابق، ص٤٦٤.

(٢) لمشاهدة الفيديو:
https://www.youtube.com/channel/UCi38HMIvRpGgMJ0Tlm1WYdw

(3) Noah Giansiracusa: How Algorithms Create and Prevent Fake News: Exploring the Impacts of Social Media, Deepfakes, GPT-3, and More, r, Apress Media, 2021, p52
&Jane Lytvynenko: «A Belgian Political Party Is Circulating A Trump Deepfake Video,» BuzzFeed News, May 20, 2018: https://www.buzzfeednews.com/article/ janelytvynenko/a-belgian-political-party-just-published-a-deepfakevideo.

(4) KOENIG Gaspard:«Les «deep fakes» ou la fin du débat démocratique», Les Échos, Éditos & Analyses, 16 octobre 2019: https://www.lesechos.fr/ideesdebats/editos-analyses/les-deep-fakes-ou-la-fin-du-debat-democratique1140377

(5) 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-videozelenskyy-experts-war-manipulation-ukraine-russi

CE Noticias Financieras English: «Reality VS fake news and deep fakes created by artificial intelligence»., February 6, 2023 Monday. advance.lexis.com/api/document?collection=news&id=urn:contentItem:67GW-R3M1-JCG7-8117-00000-00&context=151683. Accessed February 14, 2023.

٤- التشهير والانتقام الإباحي وابتزاز الآخرين:

لعلَّ هذا هو أشهر استخدامات تقنية التزييف العميق، ويتحقق عن طريق القيام بفبركة الفيديوهات للأشخاص، وتسمى هذه العملية بالتزييف الإباحي العميق. ولمعرفة مدى استخدام تلك التقنية في التشهير والابتزاز للأفراد نستعرض إحصائيَّة لموقع «Start Deep Trace»؛ حيث عثر هذا الموقع ووثق وجود ١٤٦٧٨ فيديو مزيف بواسطة تقنية التَّزييف العميق سنه ٢٠١٩ منها ٩٦٪ كانت للمواد الإباحية[١].

ومن المؤكد أن تلك السلبيات تؤدي إلى العديد من المخاطر، وأهمها:

١- فقدان المصداقية:

لا شك أن انتشار الفيديوهات المزيفة والأخبار غير الصحيحة يؤدي إلى زعزعة المصداقية لدى الأفراد، ويغذي الشكّ في كل ما يعرض لهم على وسائل التواصل الاجتماعي؛ وهو ما يهدد استقرار وانسجام المجتمع ويسهم في نشر الإشاعات[٢].

٢-الإضرار بالحياة السياسية:

لقد أكدت لنا التجربة أنه كلما اقتربت الانتخابات زادت الإشاعات، وخاصة بعد ظهور تقنية التَّزييف العميق، فهذا تقرير لجامعة (أكسفورد) البريطانية يقرر أن ما يقارب ٢٥٪ من الفيديوهات حول الانتخابات الفرنسية كانت مُزَيَّفَة وليس لها أساس من الصحة[٣]، لذا صنفت تلك التقنية بأنها من ضمن أعلى ثمانية تهديدات في الانتخابات الأمريكية عام ٢٠٢٠ [٤].

٣- تدمير الحياة بالتسبب في الفضائح الإباحية:

لعلَّ قيام الأفراد بِنَشْرِ صورهم الشخصية على صفحات الإنترنت بإرادتهم يكون رائده مشاركة لحظاتهم السعيدة مع الآخرين أو حفظ صورهم، إلا أنهم بعد ذلك قد يجدونها مركبة على فيديوهات إباحية، وهذه الجريمة سُمِّيَتْ (بالانتقام الإباحي

(1) 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-saysnearly-96-of-deepfake-v

(٢) د. أحمد الخولي: مرجع سابق، ص ٢٥٧.

(٣) د. شريف اللبان: تكنولوجيا النشر الصحفي، الاتجاهات الحديثة، الدار المصرية اللبنانية، ٢٠٠١، ص٢٦٠.

(٤) ماري شروتر: مرجع سابق، ص١٧.

'Revenge porn') وقد أدت هذه الجريمة إلى العديد من حالات الانتحار، فقد انتحرت فتـاة في أستراليـا عام ٢٠١٨، بعدمـا تمَّت سرقـة صورها وتركيبها علـى فيديوهات وصور إباحية[١]، كما انتحرت فتاة مصرية (١٦ عامًا) في يناير ٢٠٢٢ بعدما قام أحد الأشخاص بالحصول على صورها من أحد تطبيقات التواصل الاجتماعي، وقام بتكوين فيديو مزيف لها[٢].

والواقع أن هذه المخاطر لها ثلاثة أسباب رئيسية، هي:

- **الأول:** توافـر البيانات الشخصية والصور علـى مواقع التواصل الاجتماعي؛ ممَّا يسهل أخذها وتزييفها.
- **الثاني:** تواجد التطبيقات الخاصة بالتزييف العميق حتى صارت في متناول الجميع.
- **الثالث:** أنه لم تعُد هناك حاجة إلى الاحترافية؛ حيث إنَّ هذه التطبيقات أصبحت متاحة وسهلة الاستخدام من قبل العامة ولا تحتاج إلى مُبرمجين[٣].

(1) Ally Foster: Picture Reveals Sickening Online Secret, NEWS.COM.AU -JUNE 30, 2018
Image based abuse: Picture reveals sickening online secret | news.com.au — Australia's leading news site
Desai: «Smile for the Camera: The Revenge Pornography Dilemma, California's Approach, and Its Constitutionality», Hastings constitutional law quarterly, vol. 42,2015, p.464

(٢) ولعلَّ هذه الفتاة كانت صاحبة رسالة مؤثرة وهي تكتب آخر كلماتها أنها ليس تلك الفتاة التي نشرها المجرمون
https://www.masrawy.com/news/news_regions/details/2022/1/10/2156130/%D8%A8%D8%B3%D9%86%D8%AA-%D9%81%D8%AA%D8%A7%D8%A9-%D8%A7%D9%84%D8%BA%D8%B1%D8%A8%D9%8A%D8%A9-%D9%82%D8%B1%D8%A7%D8%B1-%D8%AC%D8%AF%D9%8A%D8%AF-%D9%84%D9%84%D9%86%D9%8A%D8%A7%D8%A8%D8%A9-%D8%A8%D8%B4%D8%A3%D9%86-6-%D9%85%D8%AA%D9%87%D9%85%D9%8A%D9%86-%D9%81%D9%8A-%D9%88-%D8%A7%D9%82%D8%B9%D8%A9-%D8%A7%D9%84%D8%B5%D9%88%D8%B1-%D8%A7%D9%84%D8%B9%D8%A7%D8%B1%D9%8A%D8%A9-

(٣) د. محمـود سلامـة عبد المنعم: جريمة الانتقـام الإباحي عبر تقنية التزييف العميق والمسؤوليـة الجنائية عنها، المجلد٢، ع ٢، ٢٠٢٢، ص٣٧٢.

المبحث الثاني

التمييز بين التَّزييف السطحي والتزييف العميق

ينقسم المحتوى المزيف إلى إحدى صورتين[١]: الصورة الأولى: التزييف السطحي أو البسيط، والصورة الثانية: التزييف العميق.

الصورة الأولى- التَّزييف السطحي أو البسيط (cheap fake) (shallow fakes)[٢]:

يتحقق التزييف السطحي أو البسيط بإحدى الوسائل الآتية:

١- استخدام تقنيات لتعديل نبرة الصوت دون تعديل في أساسيات الفيديو؛ وذلك بغرض ترك انطباع سيء لدى المتلقين لهذا الفيديو[٣].

٢- التلاعب بتاريخ وموقع إصدار المقطع حتى يظهر بصورة مغايرة للواقع؛ سواء من حيث المكان، أو من حيث التاريخ. ومن الأمثلة المبكرة لذلك: التلاعب بالصورة الأيقونية (لإبراهام لينكولن) عام ١٨٦٠. فعلى الرغم من أن تلك الصورة تبدو أصلية، إلا أنها عبارة عن مزيج من صور فوتوغرافية لرأس لينكولن وجسد جون كالهون، ومن الأمثلة على ذلك أيضًا ما حدث مع (ميلارد تايدينجز) الذي خسر محاولة إعادة انتخابه في عام ١٩٥٠ لمجلس الشيوخ الأمريكي؛ بسبب صورة تمَّ التلاعب بها أظهرته -على غير الحقيقة- يتحدث مع زعيم الحزب الشيوعي.

---

(١) دليل التزييف العميق: البرنامج الوطني للذكاء الاصطناعي، الجمهورية الأردنية، يوليو ٢٠٢١، ص٨.

(2) Noah Giansiracusa: How Algorithms Create and Prevent Fake News: Exploring the Impacts of social media, Deepfakes, GPT-3, and More, r, Apress Media, 2021, p42

(٣) نجد أنه قد تم استخدام تقنية التزييف السطحي في عام ٢٠١٩ لفيديو للمتحدثة الرسمية لمجلس النواب الأمريكي Nancy Pelosi قد تم إبطاء الفيديو إلى خمس وسبعين بالمائة مما أظهرها وكأنها تتحدث وهي مخمورة وانتشر هذا الفيديو وحقق ٢,٥ مليون مشاهدة في يومين و٤٧٠٠٠ مشاركة.

Johnson Phylis, Punnett Ian: Redefining Journalism in an Age of Technological Advancements,IGI GLOBAL,p30

The Guardian, «Real v Fake: Debunking the 'drunk' Nancy Pelosi Footage,» The Guardian, May 24, 2019, https://www.theguardian.com/us-news/video/2019/may/24/real-vfake-debunking-the-drunk-nancy-pelosi-footage-video

مثال آخر، ولكن في تلك المرة حدث التغيير عن طريق تسريع الفيديو وهو الحوار بين دونالد ترامب الرئيس الأمريكي وأحد الصحفيين والذي كان يحاوره وعندما تم تسريع الفيديو قبل نشره ظهر الصحفي وكأنه قام بضرب أحد العاملين باليد

&James J. F. Forest: Digital Influence Warfare in the Age of social media (Praeger Security International), Praeger Publishers Inc, 2021, p77

Sarah Sanders: «We Stand by Our Decision to Revoke This Individual's Hard Pass. We Will Not Tolerate the Inappropriate Behavior Clearly Documented in This Video,» Twitter, accessed December 8, 2022, https://twitter.com/PressSec/status/1060374680991883265Top of FormBottom of Form

ويُعـد برنامـج تحريـر الصـور الشهـير (Photoshop) هـو حاليًـا المثال الأكـثر شهرة لتكنولوجيـا معالجة الصـور. فقد تمَّ اختراع (Photoshop 50) لأول مرة في عام ١٩٨٧ وتمَّ نشـره على نطاق واسع بحلول عام ١٩٩٠. واليوم، يُعـد Photoshop أداة معروفة في ترسانة الصور، ويستخدم للتلاعب بكل شيء من أغلفة المجلات إلى منشورات Instagram.... إلخ.

وعلى الرغم من وجود تاريخ أطول من التلاعب بالصور، إلا أن التلاعب بالفيديوهات له أيضًا تاريخ طويل، حيث شهدت سنة ١٩٧٠ بداية الرسوم المتحركة، وذلك باستخدام صور 2D لإنشاء تأثيرات بصرية. ومع ذلك، فإنَّ هذه التطبيقات لا تقارن بواقع التَّزييف العميق والمنطق التقني الكامن وراءها؛ حيث تجمع تقنية التزييف العميق بشكل أساسي بين تقنية القص واللصق وتوليد الصور[١].

وبالإمعـان فيما تقدم؛ نجد أن التَّزييف السطحي يعني التلاعب في الصور ويسمى (Photoshopping)[٢]، وتسريـع وتبطـيء الفيديوهات، ونجـد أن هذه التقنية ظهرت في منتصف العقد الأول من القرن الحادي والعشرين؛ حيث أصبح الوصول إلى برامج الفوتوشوب وأدوات التحرير الرقمية أكثر سهولة[٣].

ومن ضمن وسائل التَّزييف السطحي إعادة صياغة السياق (Re-contextualizing) وتحريفه. ففي إبريل ٢٠١٨ تمَّ تداول تقرير مزيف لهيئة الإذاعة البريطانية، وتمَّ تقديم

(1) Elizabeth Caldera: ««Reject the Evidence of Your Eyes and Ears»: Deepfakes and the Law of Virtual Replicants,» Seton Hall Law Review: Vol. 50: Iss. 1 , Article 5. 2019 Available at: https://scholarship.shu.edu/shlr/vol50/iss1/5 p183

(٢) هـو محـرر الرسوميات النقطية، تم إنشاؤه في عام ١٩٨٨ عن طريق توماس نول وجون نول وتم تطويره بواسطة شركة أدوبي ليواكب الأنظمة المختلفة مايكروسوفت ويندوز وماك.

وتم اعتمـاد نظـام تسمية فوتوشوب على أرقام الإصـدارات. لكن بحلول أكتوبر ٢٠٠٢ (بعد تقـديم العلامة التجارية كريتيف سويـت) تم تعيـين كل إصدار جديـد من فوتوشوب بـ «CS» بالإضافة إلى رقم، علـى سبيل المثال، الإصـدار الرئيسي الثامن مـن فوتوشـوب كان «Photoshop CS» والتاسع كان «Photoshop CS2» كما تم نشـر Photoshop CS3 إلى CS6 في إصدارين مختلفـين: قياسي وممتد. ومع تقديم العلامة التجاريـة كريتيف كلاود في يونيو ٢٠١٣؛ وبالتالي، تم تغيير اللاحقة من «CS» إلى «CC»، وتم تغيـير مخطـط ترخيص فوتوشـوب إلى نظام البرمجيات كخدمة. تاريخيًّا، تم تضمـين الفوتوشوب مع برامج إضافيـة مثـل أدوبي إيمج ريدي وأدوبـي فايروركس وأدوبي بريدج وأدوبي ديفايس سنترال وأدوبـي كاميرا رو (بالإنجليزية: Adobe Camera RAW).

Elizabeth Caldera: REJECT THE EVIDENCE OF YOUR EYES AND EARS»1: DEEPFAKES AND THE LAW OF VIRTUAL REPLICANTS, SETON HALL LAW REVIEW [Vol. 50:177]

(3) Clare McGlynn, Erika Rackley, and Ruth Houghton, «Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse,» Feminist Legal Studies 25, no. 1 (April 1, 2017): 25–46, https://doi.org/10.1007/s10691-017-9343-2

Britt Paris, Joan Donovan: DEEPFAKES AND CHEAP FAKES THE MANIPULATION OF AUDIO AND VISUAL EVIDENCE, Data & Society's Media Manipulation research initiative,p27

قصة كاذبة عن التصعيد النووي بين (الناتو) وروسيا [١] وكانت مدة ذلك المقطع أربع دقائق فقط، وبدأ الرأي العام والمشاهدون ينزعجون ممَّا قدم، إلا أن هيئة الإذاعة البريطانية أصدرت بيانًا شرحت فيه أن المقطع تمَّ تجميعه من لقطات مختلفة كونت فيديو مزيفًا [٢].

الصورة الثانية- التَّزييف العميق (Deep fakes):

هو عملية استبدال الوجه (face-swap) [٣] أو التلاعب الصوتي Deepfakes (Audio) بواسطة الذكاء الاصطناعي باستخدام خوارزميات الذكاء الاصطناعي [٤]، وتنقسم عبارة التَّزييف العميق إلى كلمتين «Deep» وهي تعني العمق نسبة إلى خوارزميات الذكاء الاصطناعي ومستمدة من التعلم العميق «Deep Learning [٥] والتعلم الآلي Machine [٦] Learning» والكلمة الثانية هي fake أي المزيفة، نسبة إلى تزييف تلك الفيديوهات [٧].

ومن أشهر التطبيقات المستخدمة لهذه التقنية: Deep، Face Swap، Fake App

(1) Martin Coulter, «BBC Issues Warning after Fake News Clips Claiming NATO and Russia at War Spread through Africa and Asia,» London Evening Standard, accessed April 25, 2018, https://www.standard.co.uk/news/uk/bbc-issues-warning-after-fake-newsclips-claiming-nato-and-russia-at-war-spread-through-africa-and-a3818466.html; «BBC Forced to Deny Outbreak of Nuclear War after Fake News Clip Goes Viral,» The Independent, April 20, 2018, https://www.independent.co.uk/news/media/bbc-forceddeny-fake-news-nuclear-war-viral-video-russia-nato-a8313896.html.

(2) Chris Bell, «No, the BBC Is Not Reporting the End of the World,» April 19, 2018, https:// www.bbc.com/news/blogs-trending-43822718

(٣) يقصد بهذا المصطلح تبديل وجه فعلى في الفيديو وهو المصدر ويتم وضع وجه آخر وهو المنتج

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

(٥) لعل مصطلح التعلم العميق: يعني قدرة الآلة أو البرنامج على التعلم التلقائي والتطور من خلال التجارب السابقة عبر تزويدها بمجموعة ضخمة من البيانات معتمدًا على الشبكات العصبية ومستوحيًا من بيولوجيا الدماغ البشرية.

«Specific form of machine learning based on neural networks – inspired by the biology of the humanbrain – which combines different layers of information».

European Parliamentary Research Service Scientific: Tackling deepfakes in European policy- STUDY Panel for the Future of Science and Technology EPRS | Foresight Unit (STOA) PE 690.039 – July 2021,p XIII

https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf

Ian Goodfellow, Yoshua Bengio, Aaron Courville: Deep Learning [draft of March 30, 2015]- MIT Press- 2016-p 20

(6) Noah Giansiracusa: How Algorithms Create and Prevent Fake News: Exploring the Impacts of Social Media, Deepfakes, GPT-3, and More, r, Apress Media, 2021,p41

«Algorithms with a certain unsupervised learning capacity. Machine learning is more advancedthan rule-based AI, and is generally based on the comparison of data rather than prior instructions. The technology relies heavily on statistics»

European Parliamentary Research Service Scientific: Tackling deepfakes in European policy- STUDY Panel for the Future of Science and Technology EPRS | Foresight Unit (STOA) PE 690.039 – July 2021,p XIII

https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf

(7) Thanh Thi Nguyena , Quoc Viet Hung Nguyenb , Dung Tien Nguyena , Duc Thanh Nguyena , Thien Huynh-Thec , Saeid Nahavandid , Thanh Tam Nguyene , Quoc-Viet Phamf , Cuong M. Nguyen: Deep Learning for Deepfakes Creation and Detection: A Survey_ p1

https://arxiv.org/pdf/1909.11573.pdf

Face Lab ولعـلَّ التساؤل المطروح الآن هو: ما آليات عمل هذه التقنية؟ وكيف يتمّ إنشاء الصور والفيديوهات؟

إن هـذه البرامـج تعمـل عـن طريـق آليـة محـددة وفقًـا لخوارزميتـين[١]: الأولى تسمـى (generator) ويتـم بموجبهـا نسخ مقطع فيديـو متطابق عن طريـق استيراد وجـه خارجـي[٢] ورصـد صور مختلفـة لحركـة الشخص وتعابـير وجهـه[٣]. و الثانية تسمـى(discriminator) وتعمـل على مراجعة جـودة الفيديو ومحاولـة استبعاد الأقل مصداقيـة والأقل جودة، ومن خـلال عملية تسمـي (Gan)[٤] أي (شبكات الخصومة التوليديـة) وهي شبكات عصبية اصطناعية (Artificial Neural Networkes)[٥] ومن ثـمَّ يتم إرجاع العديـد إلى الخوارزمية الأولى لإعادة ضبطه حتى يتـم إصدار الفيديو بشكل يبدو كالحقيقة الكاملة[٦]، ولتوضيح آلية عمل الخوارزميتين نضرب مثالاً بالمزور والخبـير الفني المختص بالكشف عن التزوير[٧]؛ حيث يبدأ المزور في عمله حتى يتقنه ولا يستطيع الخبير كشفه، وهي تلك الآلية التي تعمل بها كلتا الخوارزميتين[٨].

(1) A Beginner's Guide to Generative Adversarial Networks (GANs), PATHMIND, http://pathmind.com/wiki/generative-adversarial-network-gan (last visited Mar. 25, 2020) [https://perma.cc/LGB6-3HK3]

(٢) استخدم باحثون في جامعة كارنيجي ميلون أداة لتحديد ما إذا كان الفيديو مزيفًا من خلال تحليل نبض الموضوع. يميل نبض الفرد إلى البقاء ثابتًا، حتى في نقاط النبض المختلفة. ومع ذلك، إذا تم إنشاء مقطع فيديو عن طريق وضع طبقات من الصور ومقاطع الفيديو فوق بعضها البعض، فقد يكون لما يبدو أنه فرد واحد في مقطع فيديو مختلفًا.

Sara Ashley O'Brien: Deepfakes Are Coming. Is Big Tech Ready?, CNN BUS. (Aug. 8, 2018, 11:16 AM), https://money.cnn.com/2018/08/08/technology/deepfakes-countermeas ures-facebook-twitter-youtube/index.html

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

(٤) دليل التزييف العميق: البرنامج الوطني للذكاء الاصطناعي، الجمهورية الأردنية، يوليو ٢٠٢١، ص٦.

Generative Adversarial Networks are machine learning algorithms that can analyse a given set of images and create new images with a similar level of qualityEuropean Parliamentary Research Service Scientific: Tackling deepfakes in European policy- STUDY Panel for the Future of Science and Technology EPRS | Foresight Unit (STOA) PE 690.039 – July 2021,p XIII
https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf

(٥) الشبكـة العصبيـة: يُعرف باسم الشبكـة العصبية الاصطناعية، وهو نوع من التعلم الآلي مستوحـى من بنية الدماغ البشري. تتكون الشبكة العصبية من عقد معالجة بسيطة، أو «خلايا عصبية اصطناعية»، وهي عبارة عن نظم لمعالجة البيانات تحاكي الشبكات العصبية الطبيعية

Ad J. W. van de Gevel and Charles N. Noussair: The Nexus Between Artificial Intelligence and Economics, published by Springer, download from https://link.springer.com, 2013,p.10.

(6) Nisha Dhanraj Dewani, Zubair Ahmed Khan, Aarushi Agarwal ,Mamta Sharma, Shaharyar Asaf Khan: Handbook of Research on Cyber Law, Data Protection, and Privacy (Advances in Information Security, Privacy, and Ethics) Information Science Reference, 2022,p38

(7) Goodfellow, Ian, et al. «Generative adversarial networks.» Communications of the ACM 63.11 2020,p 139.

(8) Davey Gibian: Hacking artificial intelligence: a leader's guide from deepfakes to breaking deep learning, Rowman & Littlefield, 2022 p113

نشأته:

نشأ التزييف العميق في عام ٢٠١٧ على أحد المواقع الإلكترونية «Reddit»[١]؛ حيث تواجد به أحد الحسابات يحمل اسم « Deep fakes» وكان يعمل على تركيب فيديوهات وصور لعدد من المشاهير[٢] مستخدمًا في ذلك خوارزميات الذكاء الاصطناعي[٣]، وفي عام ٢٠١٩ استحدثت شركة سامسونج نظامًا يمكن الشخص من إنشاء مقاطع وهمية[٤]، وفي سبتمبر ٢٠١٩ أكدت هاو لي أن الصور ومقاطع الفيديو المزيفة التي تبدو حقيقية تمامًا ستكون متاحة لكافة الناس خلال عام، كما نجد أن منظمة «Deep Trace Labs» أقرت في تقريرها لعام ٢٠٢٠ أن ما يقارب من خمسين فيديو تمَّ صنعها بواسطة التَّزييف العميق، ٩, ٨٨٪ من أجل الترفيه، و٤, ٤٪ من الرياضة، و٤٪ من السياسة[٥].

وفي ٢٩ سبتمبر ٢٠١٩، تمَّ تقديم برنامج ZaoApp إلى متجر iOS في الصين. ولعلَّ Zao هو تطبيق لتبديل الوجه، ويستخدم مقاطع من مجموعة كبيرة ومتنوعة من الأفلام والبرامج التليفزيونية، ويقوم بتغيير وجه الشخصية بشكل مقنع، وذلك باستخدام صور سيلفي من هاتف المستخدم. ومن المثير أنه في غضون ثلاثة أيام كان ZaoApp التطبيق الأكثر تحميلًا في الصين والأكثر نجاحًا في تبني تقنية «التَّزييف العميق» حتى الآن: حيث يمكن إنشاء مقطع فيديو في أقل من ثماني ثوانٍ من صورة واحدة أو مقطع فيديو أو ملف GIF[٦]. بعد فترة وجيزة من إصدار ZaoApp، وقد أصدرت

---

(١) ريديت: هو مجتمع إخباري على الإنترنت، إلا أنه يعتبر من مواقع مشاركة الروابط ومناقشتها حتى بات يشبه المنتديات، يعرف ريديت بالصفحة الرئيسية للإنترنت. يستطيع الأعضاء المسجلون في الموقع إضافة الكثير من أنواع المحتوى إلى الموقع مثل الروابط والمنشورات النصية والصور، والتي يتم التصويت عليها بعد ذلك لصالح أو رفض أعضاء آخرين، التأسيس: ٢٣ يونيو ٢٠٠٥، ميدفورد، ماساتشوستس، الولايات المتحدة. https://ar.wikipedia.org/wiki/%D8%B1%D9%8A%D8%AF%D9%8A%D8%AA

(2) Mahdi Khosravy, Isao Echizen, Noboru Babaguchi: Frontiers in Fake Media Generation and Detection, Springer, 2022,p33 &Julie B. Wiest: Theorizing Criminality and Policing in the Digital Media Age, emrald,2021,p26

(٣) د. أحمد محمد الخولي: المسئولية المدنية الناتجة عن الاستخدام غير المشروع لتطبيقات الذكاء الاصطناعي، مجلة البحوث الفقهية والقانونية، أكتوبر ٢٠٢١، ص٢٥٢.
Shankar Bhawani Dayal , Brett van Niekerk: Deepfake Video Detection ,ECCWS 2021 20th European Conference on Cyber Warfare and Security,p100

(٤) د. أحمد مصطفى محرم: مرجع سابق، ص٢٥١٠.

(5) Henry Ajder: «Deepfake Threat Intelligence: a statistics snapshot from June 2020,» Sensity, July 3, 2020: https://sensity.ai/deepfake-threat-intelligence-astatistics-snapshot-from-june-2020
Rapport: The State Of Deepfakes: Landscape, Threats and Impact, Deeptrace, 27 septembre 2019, PP.1-3

(6) L He et al: 'New Chinese 'deepfake' face app backpedals after privacy backlash' (CNN Business, 3 September 2019)

الشركـة أكبر مشغل للمدفوعات عـبر الإنترنت Alipay الذي لديه ما يقرب من ١ مليار مستخدم نشط تحذيرًا مفاده أن مستخدميه يجب أن «يتأكدوا من أنه بغضّ النظر عن مدى تطور تقنية تبديل الوجه الحالية، فإنها لا يمكن أن تخدع تطبيقات الدفع الخاصة بنا[١]».

وقـد ظهر في عام ٢٠٢١ تقنية تحريك صور الموتـى وظهورهم كأنهم أحياء، وذلك مـن خـلال موقـع MyHeritage (ماي هيرتـاج)[٢]، عن طريـق استخـدام خوارزمية التعلـم العميق، ونجد أن أكثر من (١٨٠) مليون مـرة تمَّ استخدام تلك الخاصية؛ ممَّا يثبـت استخدام تلك التقنيـة بصورة واسعة المجال[٣]. بـل إنَّ العجيب أنه تمَّ استخدام تلـك التقنية لاستحضـار الموتى، مثلما فعل متحف دالي فـي فلوريدا مع الفنان الراحل «سلفادور دالي»، إذ استعان المتحف الأمريكي بهذه التقنية للسماح لزواره بالتقاط صورة حيَّة مع دالي – الذي توفى عام ١٩٨٩ – حيث يقوم بالتقاط صور سيلفي بنفسه[٤].

وقد حـدث جدال فقهي حول مشروعية استخدام تقنية التَّزييف العميق في تحريك صور الموتى، وهل يُعد انتهاكًا لحرمة الحياة؟

اختلـف فقهاء الشريعة الإسلامية حول هذه التقنية كونها أمرًا مشروعًا أم ممنوعة فاتجـه رأي منهما إلى الجواز مع وضـع قيود لذلك على ألا يشتمل الأمر على سخرية أو سوء للميت وألا يكون هناك انتهاك لخصوصيته، وأيدت دار الإفتاء المصرية ذلك الرأي حيـث صرحـت أن: «الشريعـة الإسلامية أباحـت وسائل الترفيه والترويـح عن النفس لكونـه من متطلبات الفطرة؛ إلا أن هـذه الإباحة مقيدة بألا تشتمل على سخرية أو سوء أدب[٥]؛ فـإذا كان لا مانع شرعًـا من استخدام برامج حديثة لتحريـك الصور الثابتة، بحيث تصبـح بتقنية الفيديو بدلًا من كونها ثابتة كصورة عادية، فالأصل أن هذا مباح بشـرط مراعاة خصوصية من أفضى إلى ربه بألا يشتمـل تحريك صورته على سخرية

(1) A Coleman: 'Deepfake app causes fraud and privacy fears in China' (BBC, 4 September 2019)

(2) https://www.myheritage.com/deep-nostalgia?lang=AR

(٣) تكنولوجيا الـMyHeritage Deep Nostalgia™، هي تعلم عميق لتحريك الوجوه في الصور الساكنة – MyHeritage

Micheal Lanham: From Autoencoders and Adversarial Networks to Deepfakes, Apress, Year: 2021,p35

(4) https://www.dw.com/ar/%D8%A7%D9%84%D8%AA%D8%B2%D9%8A%D9%8A%D9%81-%D8%A7%D9%84%D8%B9%D9%85%D9%8A%D9%82-%D9%87%D9%83%D8%B0%D8%A7-%D9%8A%D9%85%D9%83%D9%86%D9%83-%D8%A7%D9%83%D8%AA%D8%B4%D8%A7%D9%81-%D9%81%D8%A8%D8%B1%D9%83%D8%A9-%D8%A7%D9%84%D8%B5%D9%88%D8%AA-%D9%88%D8%A7%D9%84%D8%B5%D9%88%D8%B1%D8%A9/a-60342217

(٥) تمت الزيارة يوم ٢٠٢٢/١٢/١٥ الساعة ٥:٢٢ صباحًا https://www.elwatannews.com/news/details/5370884

أو سوء أدب مع الميت، وبشرط ألا يؤدي ذلك إلى تدليس أو ضرر بالغير؛ وذلك كما لو ترتب على صورة المستخدم حقوق أو واجبات تستوجب بيان صورته الحقيقية لا الصورة المعدلة».

إلا أنه اتجه رأي مخالف لذلك يمثله الشيخ عبد الحميد الأطرش، رئيس لجنة الفتوى الأسبق بالأزهر الشريف أكد على «عدم جواز ذلك من الناحية الشرعية وأن هناك مخالفة في استخدامه. فهذا البرنامج يدخل في باب التمثيل بالموتى، ولا يجوز التمثيل بالموتى بأي حال من الأحوال؛ لأنَّ الإنسان كرمه الله من فوق سبع سماوات، فقال الله تعالى ﴿ولقد كرمنا بني آدم﴾، فينبغي أن تظل صورة الإنسان مكرمة متروكة كما كانت، وما دام الإنسان قد لقى ربه فينبغي أن تحفظ صورته ومكانته ولا تعرض لمثل تلك المهارات التي تظهر على السوشيال ميديا وما شابه ذلك، فلا يجوز وضع صورة المتوفى على جسد شخص آخر، كذلك لا يجوز الإتيان بصورته القديمة لوضعها في تطبيق لصنع فيديو كأنه حاضر لمناسبة حالية، فهذا ليس احترامًا للميت، ويجب الحذر من تقنية التَّزييف العميق وصنع مقاطع فيديو تستخدم تقنية الذكاء الاصطناعي، لإعداد صور أو فيديو للميت في مناسبة حالية[١]».

ونجد أن القانون المصري لم يُجرِّم مثل هذه الأفعال؛ حيث جاء نص المادة (٢٦) من قانون رقم ١٧٥ لسنه ٢٠١٨ على: «يُعاقب 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 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»[٢]. بالإمعان نجد أن القانون المصري حصرها في كلمة الغير، فمن ثمَّ يخرج الموتى عن مفهوم الغير؛ ومن ثمَّ يخرج التعدي على الحياة، كما أن التَّزييف العميق يهدف إلى الانتقام أو التشهير وهو ما لا يتحقق في حالة الموتى[٣].

(1) https://www.elwatannews.com/news/details/5367689

(٢) للاطلاع على نصوص القانون: https://www.cc.gov.eg/legislation_single?id=386006

(٣) د. محمود سلامة عبد المنعم: مرجع سابق، ص٣١.

ولقـد أثار التَّزييف العميق من خلال التطبيقات المتاحـة للجمهور عددًا من الأسئلة القانونيـة والاجتماعيـة والأخلاقيـة. هـل أي تدخل قانـوني ضـروري؟ أم يجب حظر المنتجـات المزيفـة العميقة تمامًا؟ وإذا كان للمنظمين أن يتدخلـوا، فما الطريقة الأكثر فعاليـة لتوجيـه كيفية قيام المجتمعات عـبر الإنترنت بإنشاء تزييـف عميق؟ هل ينبغي فرض أي التزامات على مشغلي المنصات؟

وفـي تطور ملحوظ اتخذت بعض مواقع الويب خطوات هامشيـة لضمان عدم إنشاء التَّزييـف العميق بصور الأفراد غير الموافقين، مثل موقع Reddit، كما حظرت subreddit الفيديوهـات المكونة عبر التَّزييف العميق؛ حيث كان لديها مائة ألف عضو[١]. وقام موقع Discord بإيقاف تشغيل خادمين تركزت الدردشات فيهما على التَّزييف العميق، وحظرت Twitter العديد من المستخدمين لديها قاموا بإنشاء مقاطع فيديو مزيفة عميقة.

ومع ذلك، فإنَّ المواقع الإلكترونية التي تستضيف مقاطع الفيديو هذه محمية بموجب قانون عام ١٩٩٦، وهو قانون آداب الاتصالات الأمريكي، وذلك في المادة (٢٣٠) حيث جـاء نصهـا كالتي: «لا يتحمل أي مقدم أو مستخدم لخدمـة كمبيوتر تفاعلية المسؤولية بسبب: (أ) أي إجراء يتخذ طوعًا بحسن نية لتقييد الوصول إلى المواد التي يعتبرها المزود أو المستخدم فاحشة أو بذيئة أو فاسقة أو قذرة أو عنيفة بشكل مفرط أو مضايقة أو غير مقبولـة بأي شكل آخـر، سواء كانت هذه المواد محمية دستوريًّا أم لا؛ أو (ب) أي إجراء يتمّ اتخاذه لتمكين أو إتاحة الوسائل التقنية لمقدمي محتوى المعلومات أو غيرهم لتقييد الوصول إلى المواد الموصوفة في الفقرة (١)[٢]». بذلك يكون قد تحصن مقدم الخدمة على هذه المواقع من أن يكون مسؤولًا قانونًا عن المحتوى الذي ينشئه المستخدمون[٣].

(1) Samantha Cole: Targets of Fake Porn Are at the Mercy of Big Platforms, MOTHERBOARD (Feb. 5, 2018), https://motherboard.vice.com/en_us/article/ 59kzx3/targets-of-fake-porn-deepfakes-are-at-the-mercy-of-big-platform

(2) § 230(c)(1) («No provider or user of an interactive computer service shall be held liable on account of- (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).»

(3) Damon Beres: Pornhub Continued to Host 'Deepfake' Porn with Millions of Views, Despite Promise to Ban, MASHABLE (Feb. 12, 2018), https://mashable.com /2018/02/12/pornhub-deepfakes-ban-not-working/ #cO19rvp..PqM.

المبحث الثالث
خصائص تقنية التَّزييف العميق

للتزييف العميق عدة خصائص، أهمها:

- الخاصية الأولى: سلوك متعلق بالذكاء الاصطناعي.
- الخاصية الثانية: سلوك متتابع النشاط.
- الخاصية الثالثة: سلوك ذات طابع دولي.

وسوف نوضح ذلك بشيء من التفصيل على النحو التالي:

الخاصية الأولى- سلوك متعلق بالذكاء الاصطناعي:

ظهر مصطلح الذكاء الاصطناعي في أول مرة في مؤتمر موث كوليدج في كلية دارموث (Dartamouth College) عام١٩٥٦[١]، بواسطة جون مكارثي[٢] بمدينة (هانوفر) بالولايات المتحدة[٣]، ونجحوا في كتابة كود لحل المشاكل، وقد أثار تعريف مصطلح الذكاء الاصطناعي الجدل الفقهي فعرفه البعض بأنه: «كل سلوك وخصائص تتسم بها البرامج الحاسوبية[٤] تجعلها تحاكي القدرات البشرية[٥]، وتقليد طرق

---

(١) د. وفاء صقر: المسئولية الجنائية عن الذكاء الاصطناعي، مجلة روح القوانين، ع ٩٦، أكتوبر ٢٠٢١، ص١٦.

د. محمود عبد الغني جاد المولي: الاتجاهات الحديثة في المسئولية الجنائية للكيانات التي تعمل بتقنيات الذكاء الاصطناعي، مجلة البحوث القانونية والاقتصادية، جامعة المنوفية، المجلد ٥٣، ع٣، مايو ٢٠٢١، ص٤٩٩.

(٢) وهو عالم كمبيوتر وعالم إدراكي، قام بتنظيم المؤتمر الدولي الأول حول الذكاء الاصطناعي في دارتموث، نيو هامبشاير
Stuart J. Russell and Peter Norvig: Artificial Intelligence A Modern Approach, by A Simon & Schuster Company, 1995, p.13.

(3) Russell, S. J. , Norvig, P:, Artificial Intelligence: A Modern Approach (2nd ed.), Upper Saddle River, New Jersey: Prentice Hall, 2003 p.17
Calo, R: Artificial Intelligence Policy, A Primer and Roadmap, University of California Davis Law Review, 2017, vol. 51, p.397.

(٤) د. أحمد لطفي السيد مرعي: انعكاسات تقنيات الذكاء الاصطناعي على نظرية المسئولية الجنائية (دراسة تأصيلية مقارنة) مجلة البحوث القانونية والاقتصادية، جامعة المنصورة، العدد٨٠، يونيو ٢٠٢٢، ص٢٥٦.
Wisskirchen, G: IBA Global Employment Institute Artificial Intelligence and Robotics and their Impact on the Workplace, 2017, p.10
El Kaakour, N: L'intelligence artificielle et la responsabilité civile délictuelle, Université Libanaise, Faculté de droit et des sciences politiques et administratives filière francophone, 2017, p. 6.

(5) Russell S. J., & Norvig: P., Artificial Intelligence, A Modern Approach, Pearson Education Limited, 3rd edition, 2014, p.15& Karl Manheim and Lyric Kaplan: Artificial Intelligence: Risks to Privacy and Democracy,2019,p.113 available at this site: https://www.tandfonline.com/doi/abs/10.1080/15230406.2021.1910075

- د. رامي متولي القاضي: نحو إقرار قواعد للمسئولية الجنائية والعقاب على إساءة استخدام تطبيقات الذكاء الاصطناعي، بحث مقدم إلى مؤتمر الجوانب القانونية والاقتصادية للذكاء الاصطناعي وتكنولوجيا المعلومات، كلية الحقوق، جامعة المنصورة، ص ٨٨٠.

التفكير البشرية[١]»، كما عرف بأنه: «أحد علوم الحاسب الآلي التي تعمل على استخدام أساليـب مستحدثة ومتطورة للقيام بمحاكاة الـذكاء البشري»[٢]، وأخيرًا هناك تعريف قالـت به الحكومة البريطانية و اعتمدته في الورقـة البيضاء للاستراتيجية الصناعية فـي بريطانيا؛ حيث عرفته على أنه: «التقنيـات التي لديها القدرة على أداء المهام التي يتطلب القيام بها الذكاء البشري، مثل الإدراك البصري، والتعرف على الكلام، وترجمة اللغة»[٣]، فالذكاء الاصطناعي[٤] يختلف عن البرامج الإلكترونية من حيث القدرة على العمل دون الحاجة إلى المبرمجين أو المشغلين.

(1) Manheim, K., Kaplan, L: Artificial Intelligence: Risks to Privacy and Democracy, 2019, p.113 https//papers.ssrn.com/so13/papers.cfm?abstract_id=3273016

الآن بونيـه: الذكاء الاصطناعي واقعه ومستقبله، كتب عالم المعرفة، المجلس الوطني للثقافة والفنون والآداب، الكويت، ع١٧٢، ١٩٩٣، صـ١١. & وجيـه محمد سليمان العميرين: الـذكاء الاصطناعي في التحري والتحقيق عـن الجريمة، دراسة مقارنة، مجلة الميزان، جامعة العلوم الإسلامية العالمية، المجلد ٩، ع٣، ٢٠٢٢، ص٤٥٦

(٢) د. عبـد المجيد مازن: استخدامات الـذكاء الاصطناعي في الهندسة الكهربائية، دراسة مقارنة، رسالة ماجستير، الأكاديمية العربية، ٢٠٠٩، ص١٧.

د. أحمـد لطفـي السيـد: انعكاسـات تقنيات الـذكاء الاصطناعي على نظريـة المسئوليـة الجنائية، مجلة البحـوث القانونية والاقتصادية، العدد ٨٠ سنه ٢٠٢٢، ص٢٥٦.

(3) HOUSE OF LORDS: AI in the UK, ready, willing and able, Ordered to be printed 13 March 2018 and published 16 April 2018, P.20.https://publications.parliament.uk/pa/ld201719/ldselect/ldai/100/10002.htm

(٤) ويمكن تقسيم أنواع الذكاء الاصطناعي إلى ثلاثة أنواع رئيسية حسب رد الفعل، وذلك على النحو التالي:

١- الذكاء الاصطناعي الضيق (Narrow AI): وهذا هو أبسط أشكال الذكاء الاصطناعي، ويتم برمجته لعمل وظيفة معينة ومحـددة، ويعتـبر تصرفه ناتجًا عن رد فعل لموقف معين، ومن الأمثلة على ذلك الروبوت «ديب بلو» (Deep Blue) والذي قامت بصنعه شركة IBM، وهو من قام بهزيمة (جاري كاسباروف) بطل الشطرنج العالمي في عام ١٩٩٦م.

٢- الذكاء الاصطناعي القوي (General AI): وهو الذي يتميز بالقدرة على جمع المعلومات والعمل على تحليلها وفقًا لخبرات ناتجـة عن مواقـف تم اكتسابها، وتؤهلـه لاتخاذ قرارات ذاتيـة، وعلى سبيل المثـال السيارات ذاتية القيـادة، وروبوتات الدردشة الفورية.

٣- الذكاء الاصطناعي الخارق (Super AI): وهي النماذج التي لا تزال تحت التجربة وتهدف لمحاكاة ذكاء الإنسان وقدرته، حيـث تقـدر هذه الروبورتات التعبير عمـا بداخلها، وأن تتنبأ بمشاعـر الآخرين، وتتفاعل معها، وهـي الجيل القادم من الآلات فائقة الذكاء.

https://futureuae.com/ar/Mainpage/Item/3063/%D8%AA%D9%87%D8%AF%D9%8A%D8%AF%D8%A7%D8%AA-%D8%B0%D9%83%D9%8A%D8%A9-%D9%85%D8%AE%D8%A7%D8%B7%D8%B1-%D8%AE%D8%B1%D9%88%D8%AC-%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A1-%D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9%D9%8A-%D8%B9%D9%86-%D8%A7%D9%84%D8%B3%D9%8A%D8%B7%D8%B1%D8%A9-%D8%A7%D9%84%D8%A8%D8%B4%D8%B1%D9%8A%D8%A9

د. محمـود محمـد سويف: جرائم الـذكاء الاصطناعي (المجرمون الجـدد)، دار الجامعة الجديـدة، ٢٠٢١، ص٢١ & أ.عمر محمد منيب: المسئولية الجنائية الناتجة عن أعمال الذكاء الاصطناعي، رسالة ماجستير، كلية القانون، قطر، ٢٠٢٣، ص٢٤.

الخاصية الثانية- التزييف العميق سلوك متتابع النشاط:

تتسم الجرائم الناتجة عن التزييف العميق بتتابع النشاط؛ حيث إنَّ الفيديوهات المزيفة لا تتمّ إلا بعد عملية رصد وتتبع للصور والفيديوهات المنشورة من قبل المجني عليه، ثمَّ العمل على تحريف تلك الفيديوهات، والتلاعب بها، واستخدامها في ابتزاز ومساومة المجني عليه، ثمَّ نشرها[١]، ومن ثمَّ فإنَّ تلك الأنشطة تُشكل -مجتمعة- الجرم ولا يكون أيٌّ منهما منفردًا مشكلًا له، كما أن تلك الأنشطة متعاقبة؛ حيث إنَّ المرحلة الأولى، وهي جمع البيانات الشخصية[٢] هي محل للمرحلة الثانية، وهي تكوين فيديو غير صحيح ومزيف؛ وتتم هاتان المرحلتان وفقًا لخوارزميات مُعدة سلفًا، ثمَّ نأتي إلى مرحلة ثالثة وهي نشر الفيديو.

---

(١) د. محمود سلامة عبد المنعم: مرجع سابق، ص٣٨٢.

(٢) وجاء التوجيه الأوروبي رقم (١٦/٦٧٩) والذي دخل حيز التنفيذ في (٢٨ مايو ٢٠١٨)؛ في المادة الرابعة منه ينص على أن البيانات الشخصية عبارة عن «أية معلومات تخص شخصًا طبيعيًّا محددًا أو قابلًا للتحديد، ويُعد الشخص قابلًا للتحديد متى كان يمكن معرفته بشكل مباشر أو غير مباشر، وذلك عن طريق الاسم أو رقم التعريف ومعرف الاتصال، أو من خلال عنصر أو أكثر من العناصر المميزة لهويته الفسيولوجية أو الجينية، أو النفسية أو الثقافية أو الاجتماعية»

Article 4/1 of REGULATION (EU) 2016/679 'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;
https://gdpr-info.eu/art-4-gdpr/
Andrew Murray:Information Technology Law: The Law and Society-Fourth Edition-Oxford University Press-2019- p573

جاء القانون الفرنسي رقم ٧ لسنة ١٩٨٧ والمعدّل بالقانون رقم ١٠٨ لسنة ٢٠٠٤، في المادة الثانية منه ينص على أن: «يُعتبر بيانًا شخصيًّا أية معلومة تتعلق بهوية الشخص الطبيعي أو يمكنها تحديد هويته سواء بطريقة مباشرة أو غير مباشرة، سواء تم تحديد هويته بالرجوع إلى رقمه أو بالرجوع إلى أي شيء يخصه.

Law No. 2004-801 of 6 August 2004 on the protection of individuals with regard to the processing of personal data and amending Act No. 78 -17 of January 1978 relating to computers, files and documents freedoms, OJ, 7 August 2004,- LOI n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, https://www.legifrance.gouv.fr/eli/loi/2004/8/6/JUSX0100026L/jo/texte

عرّف المشرع المصري البيانات في قانون مكافحة الجرائم تقنية المعلومات رقم (١٧٥ لسنة ٢٠١٨) في المادة الأولى، بأنها: «أي بيانات متعلقة بشخص طبيعي محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر».

ووفقًا لقانون حماية البيانات الشخصية المصري (رقم ١٥١ لسنة ٢٠٢٠) فإن المادة الأولى تعرّف 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 آخرى كالاسم، أو الصورة، أو الرقم التعريفي، أو أي محدد للهوية عبر الإنترنت).

https://www.privacylaws.com/media/3263/egypt-data-protection-law-151-of-2020.pdf

ومـن الجدير بالذكر أن مراحل القيـام بالنشاط الإجرامي لإنتاج فيديو مزيف يمرُّ بعـدد من الجرائم المختلفة فـي كل مرحلة كلها مجرمة؛ مما يعنـي أن كل نشاط منها مجرم في ذاته، وهذه المراحل هي:

المرحلة الأولى- مرحلة جمع البيانات والصور:

تشكل هذه الم

المصري ذلك الفعل وفقًا للمادة (١٤) من القانون١٧٥ لسنة ٢٠١٨ ووصفها بأنها جريمة الدخول غير المشروع؛ حيث جاءت المادة سالفة البيان على أنه: «يُعاقب بالحبس مدة لا تقـل عـن ٦ أشهر وبغرامة لا تقل عن ٣٠ ألف جنيه ولا تجـاوز ٥٠ ألف جنيه، أو بإحدى هاتـين العقوبتين، كل من دخل إلى موقع أو حسـاب خاص أو نظام معلوماتي مستخدمًا حقًّا مخولًا له، فتعدى حدود هذا الحق من حيث الزمان أو مستوى الدخول»[١]، ومن ثم فإن قيام الشخص بالدخول إلى نظام معلوماتي واستخدام الصور المنشورة والمعلومات الموجـودة بـه هو أمرٌ مجرَّمٌ في حد ذاته ومعاقبٌ عليـه، طبقًا للقانون المصري طالما تم ذلك دون رضاء المسؤول عن البيانات والصور[٢].

ويعـد مسلك التشريع المصري فـي هذا الصدد هو امتداد لما نصَّت عليه المادة (٢) من اتفاقية بودابست لمكافحة الجرائم المعلوماتية لعام ٢٠٠١[٣]؛ حيث جرى نصها على أنه «يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أية إجراءات آخرى يرى أنها ضرورية من أجل اعتبار كل ما يلي جريمة جنائية وفقًا لقانونه الداخلي الدخول المتعمد لـكل أو لجزء من نظام الحاسب الآلي بدون حق، وبنيـة إجرامية للحصول على بيانات الحاسـب أو أية نيـة إجرامية آخرى أو أن ترتكب الجريمة في حاسب آلي يكون متصلًا عـن بُعد بحاسب آخر»[٤]، ومن ثم فإن هذه الاتفاقية أقرت عدم مشروعية الدخول إلى

---

(١) راجع نصوص القانون على: https://manshurat.org/node/31487

(٢) أسامة بن غانم: جريمة الدخول غير المشروع إلى النظام المعلوماتي، مجلة دراسات المعلومات، ع١٤، ٢٠١٢، ص١٣.

(٣) هـي اتفاقيـة تمت في مدينة بودابست في سبتمبر ٢٠٠١ وقامت دول عـدة بالتوقيع عليها وهي اتفاقية مفتوحة لأي من الدول التـي ترغـب فـي الانضمام لها وانضمت لها (٢٦) دولة، فهـي على الرغم من كونها أوروبية الميـلاد إلا أنها ذات طابع دولي، د. خالد حسن أحمد لطفي: الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية / دار الفكر الجامعي، ٢٠١٩، ص٧٦.

(4) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.»Convention on Cybercrime- European Treaty Series - No. 185- Budapest, 23.XI.2001https://rm.coe.int/1680081561.

بيانات الشخص والتعرض لها، وجعلته مجرمًا، بل وتركت تحديد العقوبة وفقًا لكل تشريع[١].

وعلى صعيد التشريعات المقارنة نجد أن قانون العقوبات الفرنسي جرَّم في المادة ٣٢٣-١ منه الدخول غير المشروع على النظام المعلوماتي، وجعله معاقبًا عليه بالحبس لمدة سنتين والغرامة التي مقدارها ٦٠٠٠٠ يورو[٢].

المرحلة الثانية- مرحلة التحريف والتزييف وصنع الفيديوهات والصور:

حيث تتكون هذه المرحلة من جريمتين، وهما: ١- جريمة معالجة المعطيات الشخصية للغير. ٢- جريمة انتهاك الخصوصية دون رضا الغير. وقد نصت المادة (٢٥) من القانون المصري رقم ١٧٥ لسنة ٢٠١٨ على أنه: «يُعاقب 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 أخبارًا أو صورًا وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة»[٣].

وقد جرَّمت المادة (٢٦) من ذات القانون معالجة معطيات البيانات؛ حيث جاء نصها على أنه: «يُعاقب 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 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.

(1) Adomi, Esharenana: Security and Software for Cybercafesi- information science reference,2008, p226.

(2) Art. 323-1 Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de (L. no 2004-575 du 21 juin 2004, art. 45-I) «deux ans» d'emprisonnement et de (L. no 2015-912 du 24 juill. 2015, art. 4) «60 000 €» d'amende.

(٣) الجريدة الرسمية - العدد ٣٢ مكرر (ج) - السنة الحادية والستون، ٣ من ذي الحجة سنة ١٤٣٩هـ، الموافق ١٤ أغسطس، سنة ٢٠١٨م https://www.cc.gov.eg/legislation_single?id=386006

المرحلة الثالثة- مرحلة الغرض من التَّزييف واستخدامه في ابتزاز ومساومة المجني عليهم أو التضليل الإعلامي:

إنَّ صناعة محتوى مزيف يُعد مجرمًا وفقًا لقانون العقوبات المصري؛ حيث نصت المادة (١٧٨) من قانون العقوبات على أنه: «يُعاقب بالحبس مدة لا تزيد على سنتين وبغرامة لا تقل عن عشرين جنيهًا ولا تجاوز مائة جنيه أو بإحدى هاتين العقوبتين كل من صنع، أو حاز بقصد الاتجار، أو التوزيع، أو الإيجار، أو اللصق، أو العرض مطبوعات، أو مخطوطات، أو رسومات، أو إعلانات، أو صورًا محفورة، أو منقوشة، أو رسومًا يدوية، أو فوتوغرافية، أو إشارات رمزية، أو غير ذلك من الأشياء، أو الصور عامة إذا كانت منافية للآداب العامة».

ومن الواضح أن هذه المرحلة تتكون من جرائم مختلفة بداية من جريمة القذف، ثمَّ جريمة الابتزاز أو جريمة الانتقام الإباحي، أو التضليل الإعلامي. وسوف نوضح هذه الجرائم بإيجاز فيما يلي:

١-جريمة القذف: «هي إسناد فعل لشخص لو صحت يُسأل عنه من أسندت إليه وتستوجب عقابه أو احتقاره»[(١)]، وهو ذات التعريف المتبنى من قبل قانون العقوبات المصري في المادة (٣٠٢) منه التي جاء نصها على أنه «يُعد قاذفًا كل من أسند لغيره بواسطة إحدى الطرق المبينة بالمادة (١٧١) من هذا القانون أمورًا لو كانت صادقة لأوجبت عقاب من أسندت إليه بالعقوبات المقررة لذلك قانونًا أو أوجبت احتقاره عند أهل وطنه». ولقد عاقب المشرّع المصري على هذه الجريمة بالحبس والغرامة وذلك بنصه في المادة (٣٠٨) من قانون العقوبات حيث جاء نصها على أنه: « إذا تضمن العيب، أو الإهانة أو القذف أو السب الذي ارتكب بإحدى الطرق المبينة في المادة (١٧١) طعنًا في عرض الأفراد أو خدشًا لسمعة العائلات تكون العقوبة الحبس والغرامة معًا في الحدود المبينة في المواد ١٧٩ و١٨١ و١٨٢ و٣٠٣ و٣٠٦ و٣٠٧، على ألا تقل الغرامة في حالة النشر في إحدى الجرائد أو المطبوعات عن نصف الحد الأقصى وألا يقل الحبس عن ستة أشهر»[(٢)].

(١) د.محمد عبد الرحمن عبد المحسن: السب والقذف في التشريع الجنائي الإسلامي مقارناً بالقوانين الوضعية، دراسة مقارنة، مجلة كلية الشريعة والقانون بتفهنا الأشراف-دقهلية -مصر، ع٢٦، ٢٠٢٣، ج٣، ص٢٢٥٥.

(٢) راجع في ذلك نصوص قانون العقوبات على: https://manshurat.org/node/14677

وعلى صعيد التشريعات المقارنة نجد أن التشريع الفرنسي جرَّم جميع أشكال الاعتداء اللفظي والقذف، وذلك وفقًا للقانون رقم ٢٩/٧/١٨١٨ والمتعلق بحرية الصحافة بالنص في المادة (٢٩) على تعريف القذف بأنه: «كل اتهام أو إدعاء بفعل يجلب عدوانًا على سمعة شخص أو مجموعة أشخاص ينسب إليهم الفعل» [١]

والواقع أن الشريعة الإسلامية سبقت كل التشريعات السابقة، حيث جرمت فعل القذف حيث قال رسول الله (صلى الله عليه وسلم) في خطبة يوم النحر: «يا أيُّها النَّاسُ أيُّ يَوم هذا؟، قالوا: يَوْمٌ حَرَامٌ، قالَ: فأيُّ بَلَدٍ هذا؟، قالوا: بَلَدٌ حَرَامٌ، قالَ: فأيُّ شَهْرٍ هذا؟، قالوا: شَهْرٌ حَرَامٌ، قالَ: فإنَّ دِماءَكُمْ وأَمْوَالَكُمْ وأَعْرَاضَكُمْ عليكُم حَرَامٌ، كَحُرْمَةِ يَومِكُمْ هذا، في بَلَدِكُمْ هذا، في شَهْرِكُمْ هذا، فأعَادَهَا مِرَارًا، ثمَّ رَفَعَ رَأْسَهُ فَقالَ: اللَّهُمَّ هلْ بَلَّغْتُ، اللَّهُمَّ هلْ بَلَّغْتُ - قالَ ابنُ عَبَّاس رَضيَ اللَّهُ عَنْهمَا: فَوَالَّذي نَفْسي بيَدِه، إنَّهَا لَوَصيَّتُهُ إلى أمَّتِه، فَلْيُبَلِغِ الشَّاهِدُ الغَائِبَ، لا تَرْجِعُوا بَعْدِي كُفَّارًا، يَضْرِبُ بَعْضُكُمْ رِقَابَ بَعْضٍ» [٢]

٢- الابتزاز الإلكتروني: يعرف الابتزاز الإلكتروني(Cyber-Extorsion) بأنه «الضغط الممارس من شخص على آخر لدفعه لاقتراف شيء غير مشروع، سواء كان ذلك الضغط ممارسًا شفهيًّا أو كتابةً، وقد يلحق ضررًا بماله أو بنفسه، أو بمال للغير أو بنفسه إذا كان هذا الغير له علاقة بالضحية[٣]، ويتم باستخدام الإمكانيات التكنولوجية الحديثة[٤]».

بينما يعرف الانتقام الإباحي Revenge Pornبأنه: «نشر صورة، أو أكثر، أو تسجيل مرئيّ، أو صوتيّ لشخص يحمل الطابع الجنسي، ويستوي أن يكون قد تحصَّل على أيٍّ

(1) Toute allégation ou imputation d'un fait qui porte atteinte à l'honneur ou à la considération de la personne ou du corps auquel le fait est imputé est une diffamation. La publication directe ou par voie de reproduction de cette allégation ou de cette imputation est punissable, même si elle est faite sous forme dubitative ou si elle vise une personne ou un corps non expressément nommés, mais dont l'identification est rendue possible par les termes des discours, cris, menaces, écrits ou imprimés, placards ou affiches incriminés.
Toute expression outrageante, termes de mépris ou invective qui ne renferme l'imputation d'aucun fait est une injure.»https://www.legifrance.gouv.fr/loda/id/LEGITEXT000006070722

(٢) صحيح البخاري: كتاب الحج، باب الخطبة أيام منى، رقم ١٧٣٩.

(٣) د. محمد سعيد عبد العاطي و د. محمد أحمد المنشاوي: دور القانون الجنائي في حماية الطفل من الابتزاز الإلكتروني، مجلة البحوث الفقهية والقانونية، كلية الشريعة والقانون بدمنهور، ع٣٦، أكتوبر ٢٠٢١، ص١٣٥.
د. حسن حماد حميد: جريمة الابتزاز الإلكتروني، دراسة مقارنة، مجلة دراسات البصرة، العدد٤٢، ٢٠٢١، ص٥٢.

(٤) د. محمود رجب فتح الله: الأدلة الجنائية في جرائم الابتزاز الإلكتروني، مجلة الدراسات القانونية والاقتصادية، جامعة السادات، المجلد٨، ع٢، يونيو ٢٠٢٢، ص١٩.

مما تقدم برضا الشخص أو بدون رضاه»[١].

ولقـد جـرَّم المشرّع المصري في المادة (٢٦) من القانـون الصادر لمكافحة الجريمة المعلوماتية (١٧٥ لسنة ٢٠١٨) استعمال أية معلومات أو نظام معلوماتي لغرض التشهير بشخـص وربطـه بمحتوى منافٍ للآداب؛ حيـث جاء نص هذه المادة علـى أنه: «يُعاقب بالحبس مدة لا تقل عن سنتين ولا تجاوز خمس سنوات وبغرامة لا تقل عن مائة ألف جنيه ولا تجـاوز ثلاثمائة ألف جنيه أو بإحدى هاتين العقوبتين كل من تعمد استعمال برنامج معلوماتـي أو تقنيـة معلوماتيـة في معالجة معطيـات شخصية للغـير لربطها بمحتوى منـافٍ للآداب العامـة، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه»[٢]، كمـا جاءت المادة٣٠٩ مكررًا (أ) مـن قانون العقوبات المصري بالنص على أن: «يُعاقب بالحبس كل من أذاع أو سهل إذاعـة أو استعمل ولو في غير علانية تسجيلًا أو مستندًا متحصـلًا عليه بإحدى الطرق المبينة بالمادة السابقة أو كان بغير رضاء صاحب الشأن. ويُعاقـب بالسجـن مدة لا تزيد على خمـس سنوات كل من هدد بإفشـاء أمر من الأمور التـي تمَّ التحصـل عليها بإحـدى الطرق المشـار إليها لحمل شخص علـى القيام بعمل أو الامتنـاع عنه. ويُعاقب بالسجن الموظف العام الـذي يرتكب أحد الأفعال المبينة بهذه المادة اعتمادًا على سلطة وظيفته. ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها ممَّـا يكون قـد استخدم في الجريمـة أو تحصل عنهـا، كما يحكم بمحـو التسجيلات المتحصلة عن الجريمة أو إعدامها»[٣].

كمـا جـاءت المادة(٣٢٧) من قانـون العقوبات أيضاً بالنص علـى أنه: «كل من هدد غـيره كتابـة بارتكاب جريمة ضـد النفس أو المـال معاقب عليها بالقتـل أو السجن المؤبد أو المشدد أو بإفشاء أمور مُخدشة بالشرف، وكان التهديد مصحوبًا بطلب أو بتكليف بأمر يُعاقب بالسجن». ويُعاقب بالحبس إذا لم يكن التهديد مصحوبًا بطلب أو بتكليف بأمر.

وكل مـن هدد غـيره شفهيًّا بواسطة شخص آخر بمثل ما ذكـر يُعاقب بالحبس مدة

---

(١) د. حسام محمد السيد: المواجهة الجنائية لظاهرة الثأر الإباحي، دراسة مقارنة بين النظامين الأنجلو أمريكي واللاتيني، ج١، مجلة الدراسات القانونية والاقتصادية، جامعة السادات، مج٥، ع٢، ٢٠١٩، ص٢٣.

(٢) الجريدة الرسمية - العدد ٣٢ مكرر (ج) - السنة الحادية والستون، ٣ من ذي الحجة سنة ١٤٣٩هـ، الموافق ١٤ أغسطس سنة ٢٠١٨م. https://www.cc.gov.eg/legislation_single?id=386006

(٣) نص المادة ٣٠٩: https://masaar.net/egypt_laws/%D8%A7%D9%84%D9%85%D8%A7%D8%AF%D8%A9-309-%D9%85%D9%83%D8%B1%D8%B1-%D8%A3/

لا تزيد على سنتين أو بغرامة لا تزيد على خمسمائة جنيه سواء أكان التهديد مصحوبًا بتكليف بأمر أم لا. وكل تهديد سواء أكان بكتابة أم شفهيًّا بواسطة شخص آخر بارتكاب جريمة لا تبلغ الجسامة المتقدمة يُعاقب عليه بالحبس مدة لا تزيد على ستة أشهر أو بغرامة لا تزيد على مائتي جنيه»[١].

كما جرَّم المشرع الفرنسي أيضًا هذه الأفعال؛ حيث جاءت المادة (٣١٢-١٠) من قانون العقوبات الفرنسي تنصُّ على أن: «الحصول عن طريق التهديد بكشف أو ادعاء وقائع من شأنها أن تضرَّ بالسمعة والشرف يُعاقب على ذلك الابتزاز بالسجن خمس سنوات وغرامة ٧٥٠٠٠يورو»[٢].

وجاءت المادة(٢٢٦-١) من قانون العقوبات الفرنسي تنصُّ على أنه: «يُعاقب بالحبس لمدة عام وغرامة قدرها ٤٥٠٠٠ يورو كل من انتهك عمدًا ألفة الحياة الخاصة للآخرين وبأية وسيلة. ١-..... ٢-بتثبيت أو تسجيل أو نقل صورة شخص في مكان خاص دون موافقته»[٣].

وجاء نص المادة ٢٢٦-٢-١ من ذات القانون على أنه: «عندما تتعلق الجرائم المنصوص عليها في المادتين ٢٢٦-١و٢٢٦-٢ بصور ذات طابع جنسي في مكان عام أو خاص، يكون الحكم السجن لمدة عامين وغرامة مقدارها ٦٠ ألف يورو، وتطبق نفس العقوبات في حالة عدم الموافقة على النشر والتوزيع»[٤].

ولعلَّ التساؤل الذي يثور الآن هو: هل هناك فرق بين الانتقام الإباحي والابتزاز الإلكتروني؟

---

(1) https://manshurat.org/node/14677

(2) ‹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 € d'amende

(3) Art. 226-1 : Est puni d'un an d'emprisonnement et de 45 000 € d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui:
1o En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel; — V. Arr. du 4 juill. 2012 ss. art. R. 226-1.
2o En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé;

(4) Art. 226-2-1 (L. no 2016-1321 du 7 oct. 2016, art. 67) 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 p ar elle-même, à l'aide de l'un des actes prévus à l'article 226-1.

للإجابة عن هذا التساؤل نتطرق إلى تعريف كل منهما، فالابتزاز الإلكتروني هو كل تهديد يقع على المجني عليه بواسطة آخرين ويوثر عليه ويتم بواسطة وسائل التكنولوجيا ويجعلـه ذلك يقوم بالإقدام على ما طلبه أو كلفه به سواء كان ذلك مباحًا أو غير مباح؛ ومـن ثمَّ فإنَّ الابتزاز مقترن بطلب[١]، ولذا إذا كان التهديد غير مقترنٍ بطلب لا يسمى ابتزازًا وإنما يكون مجرد إيذاء للغير.

ولقد عرف المشرّع الفرنسي الابتزاز الإلكتروني في المادة ٣١٢-١ من قانون العقوبات هنـاك بأنه: «الحصول على شـيء بالعنف، أو التهديد، أو التعهد، أو التخلي، أو الكشف عن سر، أو تحويل أموال، أو أوراق مالية»[٢].

- **أما جريمة الانتقام الإباحي فتعرف بأنها:** «نشر واحدة من الصور، أو التسجيلات المرئية، أو الصوتية، تحمل الطابع الجنسي دون موافقة صاحبها ورضاه حتى ولو كانت هذه الصور قد تمَّ التقاطها في الأصل برضاه»[٣].

وبناءً على ما تقدم؛ يكون هناك اختلاف واضح بين جريمة الابتزاز الإلكتروني وبين جريمة الانتقام الإباحي، وذلك من حيث الركن المادي لكل منهما ومن حيث الغرض من الجريمة، ومن حيث الوسيلة المستخدمة، وذلك على النحو التالي:

- **الركـن المادي:** فـي جريمة الابتزاز الإلكـتروني يكون التهديد هـو المكون للركن المـادي لها وهو سابق علـى مرحلة القيام بالنشر والمشاركـة[٤] وذلك على عكس جريمة الانتقام الإباحي؛ حيث إنَّ النشر والتوزيع هو الركن المادي المكون لها.
- **ومـن حيث الغرض:** فـإنَّ الابتزاز الإلكتروني دائمًا وأبـدًا مصحوب بطلب سواء كان ذلـك ماديًـا أو معنويًـا [٥] على عكـس الانتقام الإباحي والتـي بموجبها يقع

(١) د. تامر صالح: الابتزاز الإلكتروني، دراسة تحليلية مقارنة، دار الفكر والقانون، ٢٠٢١، ص٤٠.

(2) 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 € d'amende.

(٣) د. حسام محمد أحمد: مرجع سابق، ص٣٣.

(٤) د. محمد سعيد عبد العاطي محمد: مرجع سابق، ص١٤٥.

(٥) د.هالـة عبـد المحسـن شتا: الابتـزاز الإلكتروني بـين التجريم والعقاب فـي الفقه الإسلامـي، مجلة كلية الشريعـة والقانون بالقاهرة، جامعة الأزهر، ع٤١، إبريل ٢٠٢٣، ص٤٣٥.

الضرر على المجني عليه بمجرد النشر والتوزيع والمشاركة.

- **الوسيلة:** التهديد في جريمة الابتزاز الإلكتروني يقع بأية طريقة كانت سواء كتابية أو شفهية[1]، وقد أكدت محكمة النقض ذلك؛ حيث قضت بأن: « (الركن المادى فى جريمة التهديد المنصوص عليها فى الفقرة الأولى من المادة ٣٢٧ من قانون العقوبات يتوافر إذا وقع التهديد كتابةً بارتكاب جريمة ضد النفس أو المال أو بإفشاء أو نسبة أمور خادشة للشرف، وكان التهديد مصحوبًا بطلب أو تكليف بأمر، وكان الحكم قد أورد بأسبابه قيام الطاعن بتهديد المجنى عليها عبر مواقع التواصل الاجتماعى، وتمكن من خداعها وتحصل منها على صور فى أوضاع مخلة بالحياء وهددها بنشرها، وإذ كان مصطلح الكتابة قد ورد فى المادة (٣٢٧) سالفة الذكر على سبيل البيان فى صيغة عامة لتشمل كافة وسائل الكتابة المختلفة سواء كانت بالطرق التقليدية أو بإحدى الوسائل الإلكترونية الحديثة، فإذا أثبت الحكم على الطاعن إرساله عبارات التهديد عن طريق الوسائط الإلكترونية الحديثة – وهى لوحة المفاتيح – بقصد إيقاع الخوف فى نفس المجنى عليها لحملها على أداء ما هو مطلوب منها، فإنه يكون قد استظهر الركن المادى لجريمة التهديد موضوع الاتهام، كما هى معرفة به فى القانون.

ولما كان ذلك، وكان من المقرر أن القصد الجنائى فى جريمة التهديد يتوافر متى ثبت للمحكمة أن الجاني ارتكب التهديد، وهو يدرك أثره من حيث إيقاع الرعب فى نفس المجنى عليه، وأنه يريد تحقيق ذلك الأثر بما قد يترتب عليه من أن يذعن – مرغمًا – إلى إجابة الطلب، وكان لا يلزم التحدث استقلالاً عن هذا الركن، بل يكفى أن يكون مفهومًا من عبارات الحكم وصراحة عبارات التهديد وظروف الواقعة كما أوردها، فإن النعى على الحكم بالقصور فى هذا الشأن يكون على غير أساس، ومع هذا فقد أفاض الحكم فى الحديث عن توافر القصد الجنائى فى حق الطاعن، ودلل عليه تدليلاً سائغًا ومقبولاً، ومن ثَمَّ فإن ما يثيره الطاعن من منازعة بشأن انتفاء القصد الجنائى لجريمة التهديد فى حقه ينحل إلى جدل موضوعى فى سلطة المحكمة فى تقدير الأدلة

(١) أ. سارة محمد حنش: المسؤولية الجزائية عن التهديد عبر الوسائل الإلكترونية، دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، ٢٠٢٠، ص٢٢.

واستنبـاط معتقدها مما لا يجوز الخوض فيه أمـام محكمة النقض)[١]، بينما جريمة الانتقام الإباحي العميق تتم بواسطة استخدام الذكاء الاصطناعي[٢].

- **النتيجـة:** تكـون النتيجـة فـي جريمة الابتـزاز الإلكـتروني هي الإيـذاء المادي، أو المعنـوي الذي يقع علـى المجني عليه، بينما تتحقق النتيجة في جريمة الانتقام الإباحي من تشويه سُمعة المجني عليه[٣].
- **محل الجريمة:** جريمة الابتزاز الإلكتروني لا تتقيد بالمحتوى الجنسي، وذلك على عكـس جريمة الانتقام الإباحي؛ حيث ترتبط بوجود محتوى جنسي مزيف وجودًا وعدمًا[٤].

٣- جريمة التضليل الإعلامي ونشر الشائعات: التضليل الإعلامي هو التلاعب بالرأي العـام عن طريق الإعـلام، وحاليًا يستخدم عـن طريق تطبيقـات التواصل الاجتماعي باستعمـال معلومات كاذبة أو مفبركة[٥] ويتحقق ذلك باستخدام تقنية التَّزييف العميق عـن طريـق تركيب الفيديوهات للإضـرار بالحياة السياسية، وتنص المادة ٨٠-د من قانـون العقوبات المصري على أنـه: «يُعاقب بالحبس مدة لا تقل عن ستة أشهر ولا تزيد علـى خمـس سنوات وبغرامة لا تقل عن ١٠٠ جنيه ولا تجاوز ٥٠٠ جنيه أو بإحدى هاتين العقوبتـين كل مصـري أذاع عمدًا في الخارج أخبارًا أو بيانـات أو إشاعات كاذبة حول الأوضـاع الداخلية للبـلاد، وكان من شأن ذلك إضعاف الثقة الماليـة بالدولة أو هيبتها واعتبارهـا، أو باشـر بأية طريقـة كانت نشاطًا مـن شأنه الإضـرار بالمصالح القومية للبلاد».

كمـا تنص المادة ١٠٣ مكرر-٢ من ذات القانون علـى أنه: «يُعاقب بالحبس وبغرامة لا تقـل عن خمسـين جنيهًا ولا تجاوز مائتي جنيـه كل من أذاع عمدًا أخبـارًا أو بيانات

(١) نقض جنائي؛ الطعن المقيد برقم ٢٢٨٣٠ لسنة ٨٨ قضائية.

(٢) إن الانتقـام الإباحـي يعنـي قيـام أحـد الأفراد بنشر مـا تحصل عليه مـن صور وفيديوهـات تحمل الطابـع الجنسي، وذلك بـدون رضـاه، بينما الانتقام الإباحي العميـق يقصد به نشر الفيديوهـات المفبركة والمستخدمة بواسطـة خوارزميات الذكاء الاصطناعي؛ لتشويه سُمعة الشخص.د. أحمد ذكير: مرجع سابق، ص٢٢٣٣.

(٣) د. تامر صالح: مرجع سابق، ص٢٢.

(٤) د. محمود سلامة عبد المنعم: مرجع سابق، ص٢٢.

(٥) د. أسامة عطية محمد عبد العال: المسئولية الجنائية عن جريمة التضليل الإعلامي، مجلة العلوم الاقتصادية والقانونية، ع١، السنة٦٣، يناير ٢٠٢١، ص١٥٢.

أو إشاعات كاذبة إذا كان من شأن ذلك تكدير الأمن العام أو إلقاء الرعب بين الناس أو إلحاق الضرر بالمصلحة العامة، وتكون العقوبة السجن وغرامة لا تقل عن مائة جنيه ولا تجاوز خمسمائة جنيه إذا وقعت الجريمة في زمن الحرب، ويُعاقب بالعقوبات المنصوص عليها في الفقرة الأولى كل من حاز بالذات أو بالواسطة أو أحرز محررات أو مطبوعات تتضمن شيئًا ممَّا نص عليه في الفقرة المذكورة إذا كانت مُعدة للتوزيع أو لاطلاع الغير عليها، وكل من حاز أو أحرز أية وسيلة من وسائل الطبع أو التسجيل أو العلانية مخصصة ولو بصفة وقتية لطبع أو تسجيل أو إذاعة».

ومما لا شك فيه أن تقنية التَّزييف العميق لها قدرة هائلة على إقناع الآخرين بما تمَّ تزييفه، وإقناع كافة الجمهور بما لم يقل، وما لم يتم فعله، وهذا يؤثر بشكل سلبي على الرأي العام، وهو ما يُعد تضليلًا للإعلام والرأي العام.

ولعلَّ التقدم التكنولوجي هو ما أدى إلى انتشار الأخبار الكاذبة، وجعله أمرًا سهلًا وسريع الانتشار خلال فترة زمنية قصيرة[٦]، وأصبحت الإشاعات تتزايد بشكل كبير[٧]، ونعرف الشائعة (بأنها خبر أو مجموعة من الأخبار الزائفة التي تنتشر في المجتمع بشكل سريع، ويتم تداولها بين العامة ظنًّا منهم على صحتها، ودائمًا ما تكون هذه الأخبار شيقة ومثيرة)[٨] وعرفها البعض بأنها (الأخبار التي يتناقلها الناس دون إمكانية التحقق من صحتها)[٩].

(6) Dayani, R.; Chhabra, N.; Kadian, T., & Kaushal, R.: An Exploration of Twitter Role in Rumor Propagation Among Undergraduates, Community. In Proceed-ings of the 20 th international conference on World Wide Web. 2016, P. 422

Rudat: A. Twitter Spreads Rumors: Influencing Factors on Twitter's Role in Rumor Spread Among University Students, PhD Thesis, Tubingen: Tubingen. 2015, p. 2

(7) Jiang, M., Cui, P., & Faloutsos, C.: Suspicious Behavior Detection: Current Trends and Future Directions, IEEE Intelligent Systems, 2016, 31(1), p 39.

Huang, Y. L., Starbird, K., Orand, M., Stanek, S. A., & Pedersen, H. T.: Connected Through Crisis: Emotional Proximity and the Spread of Misinformation Online, In Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing. February 2015, p. 969.

منال محمد مراد: الإشاعة طرق انتشارها ومعالجتها، رسالة ماجستير، جامعة أم درمان، ١٩٩٩، ص٢٥.

(٨) د. محمد بن عائض: الشائعات في وسائل التواصل الاجتماعي، مجلة الشمال للعلوم الإنسانية، مجلد٤، ع١، ٢٠١٩، ص١٤٤.

د. محمود رجب فتح الله: شرح قانون مكافحة الشائعات، دراسة مقارنة، دار الجامعة الجديدة، الإسكندرية، ٢٠٢٠، ص٢٦.

د. هبة بدر أحمد: الحماية الإجرائية من الشائعات «دراسة تحليلية مقارنة»، مجلة كلية الشريعة والقانون بتفهنا، ع٢٣، لسنة ٢٠٢١، ص١٩٠٦.

(٩) د. وفاء محمد صقر: المسئولية الجنائية عن بث الشائعات عبر مواقع التواصل الاجتماعي، مجلة روح القوانين، ع٩٣، إصدار يناير ٢٠٢١، ص٢٧.

د. أحمد عبد اللاه المراغي: السياسة الجنائية لمواجهة الإشاعات والأخبار الكاذبة، مجلة الدراسات القانونية، ع٥٤ ج٢، ص١٣٢٧.

وقد جرَّمها المشرّع المصري في المادة (٢٥) من قانون مكافحة تقنية المعلومات رقم ١٧٥ لسنـة ٢٠١٨ والتـي جـاء نصُّها على الآتـي: «يُعاقب بالحبس مـدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتـين، كل من اعتدى على أيّ من المبادئ، أو القيـم الأسرية في المجتمع المصري، أو انتهـك حرمـة الحيـاة الخاصـة أو أرسل بكثافـة العديد مـن الرسائـل الإلكترونية لشخصـ معين دون موافقته، أو منح بيانات إلى نظام، أو موقع إلكترونى لترويج السلع، أو الخدمـات دون موافقته، أو بالقيام بالنشر عن طريـق الشبكة المعلوماتية، أو بإحدى وسائل تقنية المعلومات، لمعلومات، أو أخبار، أو صور، وما في حكمها، تنتهك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أم غير صحيحة»[١].

كمـا جرَّمها قانـون العقوبات المصري، بنص في المادة (١٨٨) منه على أن: «يُعاقب بالحبسـ مدة لا تجاوز سنة وبغرامة لا تقل عن خمسة آلاف جنيه ولا تزيد على عشرين ألـف جنيه أو بإحدى هاتـين العقوبتين كل من نشر بسوء قصـد بإحدى الطرق المتقدم ذكرها أخبارًا أو بيانات أو إشاعات كاذبة أو أوراقًا مصطنعة أو مزورة أو منسوبة كذبًا إلى الغير، إذا كان من شأن ذلك تكدير السلم العام، أو إثارة الفزع بين الناس أو إلحاق الضرر بالمصلحة العامة»[٢].

تعقيب:

في ظلِّ غياب النصوص التجريميَّة للاستخدام غير المشروع لتقنية التَّزييف العميق، فإنـه لا بدَّ من تحديد مراحل العمـل داخل هذه التقنية «التَّزييـف العميق» واستعراض أنشطتها، حيث قد تتعدد الجرائم التي يرتكبها المستخدم لهذه التقنية سواء في قانون جرائـم تقنية المعلومـات، أو في قانون العقوبات مع مراعاة نص المادة (٣٢) من قانون العقوبـات المصـري التي تنص على أنـه : «إذا كون الفعل الواحـد جرائم متعددة وجب اعتبار الجريمة التي عقوبتها أشد والحكم بعقوبتها دون غيرها، وإذا وقعت عدة جرائم لغرض واحد وكانت مرتبطة ببعضها بحيث لا تقبل التجزئة وجب اعتبارها كلها جريمة واحدة والحكم بالعقوبة المقررة لأشد تلك الجرائم».

---

(١) انظر في ذلك قانون تقنية المعلومات على:
https://masaar.net/egypt_laws/%D8%A7%D9%84%D9%85%D8%A7%D8%AF%D8%A9-25/.

(٢) انظر في قانون العقوبات: https://manshurat.org/node/14677

الخاصية الثالثة- التزييف العميق سلوك ذو طابع دولي:

إنَّ جرائم الاستخدام غير المشروع لتقنية التَّزييف العميق من الجرائم ذات الطابع الدولي، صحيح أن مبدأ الإقليمية هو المبدأ المهيمن على تطبيق القانون الجنائي من حيث المكان، غير أن هذا المبدأ يفقد صلاحيته للتطبيق بالنسبة لجرائم تقنيات الذكاء الاصطناعي التي تتجاوز حدود المكان، فجرائم تقنيات الذكاء الاصطناعي عابرة للحدود، ولا تعرف الحدود الجغرافية، لأن الجاني في جريمة التزييف العميق قد يكون في دولة ما أو قد يكون الجناة الشركاء في الجريمة مقيمون في أكثر من دولة، ويرتكب محل الجريمة في دولة أو دول آخرى[١]، ويمكن توضيح ذلك من أكثر من زاوية، وذلك على النحو التالي:

الزاوية الأولى- طبيعة الأفعال المرتكبة:

ذلك أن السلوك الإجرامي في هذه الجريمة يقع بالاعتماد على برامج مختلفة من خلال شبكة الإنترنت التي تتسم بالعالمية[٢] والتي تؤدي إلى انتشار الفيديوهات بشكل واسع في الدول المختلفة[٣]، فهي من الجرائم التي لا تحتاج إلى وجود الفاعل على مسرح الجريمة، بل ترتكب عن بُعد[٤].

الزاوية الثانية- الاعتداء العابر للحدود:

حيث إنَّ الطبيعة الدولية لهذه الجريمة يُقصد بها أنها قد تتعرض لمصالح شخصيات في أكثر من دولة، عندئذ تؤدي إلى زعزعة الثقة العامة وفقدان المصداقية[٥]؛ ومن طبيعة شبكات الإنترنت أنها لا تخضع لحدود الزمان أو المكان، فمن السهل أن يكون المجرم في دولة والمجني عليه في دولة آخرى[٦].

---

(١) عبد الفتاح بيومي حجازي: الأحداث والإنترنت، دار الفكر الجامعي، الإسكندرية، ٢٠٠٠، ص ٢١، ا. ثيان ناصر آل ثيان: إثبات الجريمة الإلكترونية، دراسة تأصيلية تطبيقية، رسالة ماجستير، جامعة نايف العربية للعلوم الأمنية، الرياض، ٢٠١٢، ص٢٣.

(٢) أ. دعاء سليمان عبد القادر التميمي: جريمة الابتزاز الإلكتروني، دراسة مقارنة، رسالة ماجستير، جامعة القدس أبوديس، فلسطين، ٢٠١٩، ص٤٣.

(٣) ماري شروتر: الذكاء الاصطناعي ومكافحة التطرف العنيف: كتاب تمهيدي، المركز الدولي لدراسة الراديكالية، بدون تاريخ نشر، ص١٧.

(٤) د. محمد أحمد سليمان عيسى: الجهود الدولية الإقليمية لمواجهة الجرائم الإلكترونية، مجلة العلوم القانونية، جامعة عجمان، الإمارات، ع ٨، يوليو ٢٠١٨، ص١٨٢.

(٥) د. أحمد الخولي: مرجع سابق، ص٢٥٥.

(٦) أرسلاح ظفري: جريمة الاعتداء على حق الخصوصية عبر الإنترنت في الشريعة الإسلامية والنظام القانوني الأفغاني: دراسة مقارنة، مجلة ريحان للنشر العلمي، ع٢٦، ٢٠٢٢، ص١٣٩.

وقـد عالج المشرّع الفرنسي هـذه الخطورة من خلال نص المـادة (١١٣-٢-١) من قانون العقوبات، هناك والتي نصَّت على أن أية جناية أو جنحة تُرتكب عن طريق شبكة اتصـالات إلكترونيـة، أو يتم ارتكابهـا أو محاولة ارتكابها على حسـاب شخص طبيعي مقيـم على أراضـي الجمهورية الفرنسية؛ أو شخص اعتباري يقـع مقره الرئيسي فيها تعتبر وكأنها تم ارتكابها في أراضي الجمهورية الفرنسية[١].

وفي ضوء ذلك يهيب الكاتب بالمشرع المصري سلوك مسلك المشرع الفرنسي، وذلك عنـد مواجهة هذا النوع من الجرائم، ومواجهـه عقبة الحدود الناتجه عن اتساع نطاق ارتكاب الجرائم.

(1) Article 113-2-1, «Tout crime ou tout délit réalisé au moyen d'un réseau de communication électronique, lorsqu'il est tenté ou commis au préjudice d'une personne physique résidant sur le territoire de la République ou d'une personne morale dont le siège se situe sur le territoire de la République, est réputé commis sur le territoire de la République.» Création LOI n°2016-731 du 3 juin 2016 - art. 28

الفصل الثاني
التكييف الشرعي والقانوني لتقنية التَّزييف العميق

تمهيد وتقسيم:

يُمثل الذكاء الاصطناعي وتطبيقاته، والتي منها تقنية التَّزييف العميق تحديًا جديدًا للقانون من حيث مدى إمكانية تطبيق القواعد القانونية الموجودة به على المسائل القانونية المستحدثة[١] فإذا ما تم التعرض لهذه الجريمة بنصوص القانون، فيجب الوقوف أولاً على طبيعتها، وتحديد ما إذا كان استخدام تلك التقنية كأداة لارتكاب الجريمة هو بمثابة استخدام السكين في جريمة القتل أو السمّ في جريمة القتل بالسمّ، وقد يكون استخدامها في ذاته يعد مجرَّمًا[٢]؛ ومن ثمَّ نتناول في هذا الفصل التعرض لهذه المسأله في مبحثين على النحو التالى:

- **المبحث الأول: تكييف تقنية التَّزييف العميق في الفقه الإسلامي.**
- **المبحث الثاني: التكييف القانوني لتقنية التَّزييف العميق.**

(١) د. فريدة بن عثمان: الذكاء الاصطناعي مقاربة قانونية، مجلة دفاتر السياسة والقانون، مجلد ١٢، ع٢، ٢٠٢٠، ص١٥٧.

أ. عمري موسى يس بلال: الآثار القانونية المترتبة عن استخدام الذكاء الاصطناعي، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، ٢٠٢٠، ص٢٨.

(2) Sabine Gless, Emily Silver Man. Thomas WEIGEND: «If Robots cause Harm, Who is to Blame? Self-Driving Cars and Criminal Laiability», New Criminal Law Review, SSRN, Janury 29, 2016, pp.1-12.

المبحث الأول

تكييف تقنية التزييف العميق في الفقه الإسلامي

أكـدت دار الإفتاء المصرية في فتواها عـن استخدام تقنية التزييف العميق على أنه (لا يجـوز شرعًا استخـدام تلك التقنية لتَلْفِيـق مقاطع مَرْئيـة أو مسموعة للأشخاص باستخـدام الذكاء الاصطناعي لإظهارهم يفعلون أو يقولـون شيئًا لم يفعلوه ولم يقولوه فـي الحقيقـة؛ لأنَّ في ذلـك كَذِبًا وغِشًّا وإخبـارًا بخلاف الواقع، وفـي الحديث: «مَنْ غَشَّنَـا فَلَيْسَ مِنَّا»[1] (رواه مسلم)، وهو نَصٌّ قاطـعٌ صريحٌ في تحريم الغِشِّ بكل صوره وأشكالـه. فالإسلامُ إذ حثَّ على الابتكار والاختراع؛ فقد جَعَله ليس مقصودًا لذاته، بل هو وسيلة لتحقيق غَرَض ما؛ لذا أحاط الإسلامُ الابتكارات العلمية بسياج أخلاقي يقوم على أساس التقويم والإصلاح وعدم إلحاق الضرر بالنفس أو الإضرار بالغير، فمتى كان الشـيء المُخْتَرع وسيلة لأمر مشروع أخذ حكم المشروعية، ومتى كان وسيلة لأمر منهيٍّ عنـه أخذ حكمـه أيضًا. واختلاق هذه المقاطع بهذه التقنية فيـه قَصْدٌ الإضرار بالغير، وهو أمر منهي عنه في حديث النبي صلى الله وعليه وآله وسلم: «لَا ضَرَرَ وَلَا ضِرَارَ»[2]، إضافـة لما فيها مـن الترويع والتهديد لحياة الناس، والشريعـة الإسلامية جعلت حفظ الحيـاة مـن مقاصدها العظيمـة وضرورياتها المهمة؛ حتى بالغت فـي النهي عن ترويع الغير ولو بما صورته المُزَاح والترفيه[3].

وباستقـراء هذه الفتوى يتضح لنـا أن دار الإفتاء المصرية نظرت إلى تقنية التزييف العميـق على أنهـا مجرد وسيلـة وأداة ولم يجعل استعمالها محرمًا فـي ذاته، إنما تعد مجرَّمة إذا كان استخدامها بقصد ارتكاب الجريمة.

والجديـر بالذكر أن مركز الأزهـر العالمي للفتوى الإلكترونية أصـدر بيانًا مؤكدًا لذلك حيـث جاء به أن: (ما يتـم تداوله على منصات التواصل الاجتماعـي من مواقع وتطبيقات لتزييف وفبركة الصور ومقاطع الفيديوهات، والتي يوظفها بعض المستخدمين في الابتزاز

(١) صحيح مسلم، كتاب الإيمان، باب قول النبي -صلى الله عليه وسلم- (من غشنا فليس منا) رقم ١٠٢.

(٢) أخرجه ابن ماجة برقم ٢٣٤١، والدارقطني برقم ٤٥٤١ والإمام مالك في الموطأ، ج٢، ص٧٤٥ وهو حديث حسن صحيح.

(٣) فتوى صادرة من دار الإفتاء المصرية:
https://www.facebook.com/EgyptDarAlIfta/posts/pfbid02DuNdW6hvu2MXsevEAvt6PHVRMvQRyT4NrcstQCDq9h9hjkwHYoU7WcbvZxjwVt4kl

الإلكتروني بغرض جني المال أو دفع عدد من الناس قسرًا إلى أفعال منافية للآداب أو إلى جرائم جنسية، تحرّمها الأديان، وتجرّمها القوانين، وتأباها التقاليد والأعراف.

ويؤكد الأزهر أنه من المحرَّم شرعًا والمجرَّم قانونًا استخدام البرامج والتقنيات الحديثة؛ سيّما تقنية «التزييف العميق Deep Fake»، في فبركة مقاطع مَرْئية أو مسموعة أو صور لأشخاص، بغرض ابتزازهم ماديًّا أو الطعن بها في أعراضهم وشرفهم، أو دفعهم لارتكاب أفعال محرمة؛ مشددًا على أن هذه الأفعال من الإيذاء والبهتان الذي ذم الله صاحبه؛ فقال سبحانه: ﴿وَالَّذِينَ يُؤْذُونَ الْمُؤْمِنِينَ وَالْمُؤْمِنَاتِ بِغَيْرِ مَا اكْتَسَبُوا فَقَدِ احْتَمَلُوا بُهْتَانًا وَإِثْمًا مُّبِينًا﴾[١] [٢].

وبذلك يكون بيان الأزهر الشريف قد جاء متوافقًا مع فتوى دار الإفتاء المصرية، إذ جعل استخدام تلك التقنيات مجرمًا كوسيلة أو أداة لارتكاب الجريمة.

على خلاف ما سبق؛ ساق فقهاء الشريعة الإسلامية الكثير من الأدلة للتدليل على تحريم استخدام تقنية التزييف العميق، ولقد استدل الفقهاء على تحريم استعمال تلك التقنية بالقرآن الكريم، والسنة النبوية المطهرة:

أولاً- الأدلة من القرآن الكريم:

ساق فقهاء الشريعة الإسلامية للتدليل على تحريم استخدام تقنية التزييف العميق الكثير من آيات القرآن الكريم من ذلك مثلاً:

١- قوله تعالي: ﴿وَمَنْ يَكْسِبْ خَطِيئَةً أَوْ إِثْمًا ثُمَّ يَرْمِ بِهِ بَرِيئًا فَقَدِ احْتَمَلَ بُهْتَانًا وَإِثْمًا مُبِينًا﴾[٣].

حيث إنهم استنتجوا من هذه الآية الكريمة أن من يرتكب الذنب ويرمي به شخصًا آخر فهو آثم[٤]، وهذا هو ما يفعله القائم باستخدام تقنية التزييف العميق؛ حيث يقوم بتركيب وجوه أشخاص أبرياء ويلقيهم بما لا يقولون أو يفعلون.

---

(١) (الأحزاب: ٥٨).

(٢) راجع الفتوى كاملة على:
https://www.facebook.com/fatwacenter/posts/pfbid02GJwij7FuMQJDU73UHc1N3jC55S8zQnbxrsvPTk4ytvCuWkWS23v9xfDd38D2BM3ql

(٣) سورة: النساء: ١١٢.

(٤) د. مصطفى محرم: مرجع سابق، ص ٢٥٣٩.

٢- ومن ذلك أيضًا قوله تعالى: ﴿إِنَّ الَّذِينَ يُحِبُّونَ أَنْ تَشِيعَ الْفَاحِشَةُ فِي الَّذِينَ آمَنُوا لَهُمْ عَذَابٌ أَلِيمٌ فِي الدُّنْيَا وَالْآخِرَةِ وَاللَّهُ يَعْلَمُ وَأَنْتُمْ لَا تَعْلَمُونَ﴾[١].

حيث أكدوا أن ما يقوم به القائمون على التزييف العميق هو إشاعة الفاحشة والمنكر اللذيـن حذرت منهمـا الآية الكريمة، وتوعدت مرتكبيها بالعـذاب الأليم في الدنيا، بل وفي يوم القيامة.

٣- ومـن ذلك -كذلك- قوله تعـالي: ﴿وَلَا تَلْبِسُوا الْحَقَّ بِالْبَاطِلِ وَتَكْتُمُوا الْحَقَّ وَأَنْتُمْ تَعْلَمُونَ﴾[٢].

حيـث أكـد الفقهاء على أن هذه الآية الكريمة تنهى عـن التزييف وتدليس الحقائق، ومن المؤكد أن جوهر عمل تقنية التزييف العميق هو إظهار الشيء على خلاف الحقيقة، ومن ثم فهو إلباس الحق بالباطل[٣].

ثانيًا- الأدلة من السنة النبوية المطهرة:

لقد دلـل فقهاء الشريعـة الإسلامية على تحـريم استخدام تقنيـة التزييف العميق بالاستناد إلى العديد من الأحاديث النبوية، من ذلك:

قـول رسول الله صلي الله عليه وسلـم: «أَلا أُنَبِّئُكُمْ بِأَكْبَرِ الكَبائـرِ قُلْنا: بَلَى يا رَسولَ اللَّهِ، قـالَ: الإشْراكُ بـاللَّهِ، وعُقُوقُ الوالدَيْنِ، وكانَ مُتَّكِئًا فَجَلَسَ فقالَ: ألا وقَوْلُ الزُّورِ، وشَهادَةُ الزُّورِ، ألا وقَوْلُ الزُّورِ، وشَهادَةُ الزُّورِ فَما زالَ يَقولُها، حتَّى قُلتُ: لا يَسْكُتُ»[٤]

واستدلـوا من هذا الحديث الشريـف على أن تقنية التزييف العميق تشتمل على قول الزور والبهتان وأن الإفك الذي تتسبب فيه هذه التقنية يقع على كل مجني عليه.

قـول رسول الله -صلي الله عليه وسلم-: «مَن غَشَّنـا فليسَ مِنَّا»[٥]، فهذا النهي عن الغشـ يتضمن يقينًا النهي عـن استعمال تقنية التزييف العميق، حيـث إن هذه التقنية تعمل على الغش باصطناع مواقف وأفعال لم تحدث فعليًّا.

---

(١) النور: ١٩.

(٢) البقرة: ٤٢.

(٣) د. مصطفى صلاح محمد: التزييف الرقمي وأثره على حجية الأدلة الرقمية في الدعاوى الجنائية، مجلة الشريعة والقانون، القاهرة، ع ٤٠، أكتوبر ٢٠٢٢، ص٨٥٤.

(٤) صحيح البخاري: كتاب الشهادات باب ماقيل في شهادة الزور رقم ٢٦٥٤.

(٥) صحيح مسلم: كتاب الإيمان، باب قول النبي صلي الله عليه وسلم رقم ١٠١.

قول رسول الله -صلى الله عليه وسلم-: «المَكْرُ والخَديعةُ في النَّار»[١] مستخدم تقنية التزييف العميق يعمل على خداع الناس والتدليس عليهم، ومن ثَمَّ فإن عمله هذا منهي عنه.

قول رسول الله -صلى الله عليه وسلم-: « لا ضررَ ولا ضِرارَ»[٢] فهذه التقنية تهدف في صميمها وغرضها الأساسي من استخدامها السلبي إلى الإضرار بالناس وهو ما نهى الرسول الكريمة عنه في هذا الحديث الشريف.

بذلك تكون الشريعة الغراء قد أكدت على حرمة وعدم جواز استخدام تلك التقنية في الإيذاء والإضرار بالغير.

ثالثًا- القواعد الفقهية:

توجد عدة قواعد فقهية تحكم التعامل بهذه التقنية، منها:

- **درء المفاسد مقدم على جلب المصالح:**

من القواعد المسلمة في الشريعة الإسلامية أن المصلحة إذا كان في تحصيلها مفسدة مساوية لها، أو أكثر منها فيجب تركها. أي إذا تعارضت مفسدة ومصلحة فدفع المفسدة مقدم وغالب[٣] إلا ان تكون المفسدة مغلوبة؛ حيث ان الشريعة الإسلامية أمرت بترك المنهيات والاعتناء بفعل المأمورات، وذلك يأتي أولا، وجلب المنافع يأتي ثانيًا[٤]، فعن أبي هريرة رضي الله عنه قال سمعت رسول الله -صلي الله عليه وسلم- يقول: (دعوني ما تركتكم، إنما هلك من كان قبلكم بسؤالهم واختلافهم على أنبيائهم، فإذا نهيتكم عن شيء فاجتنبوه وإذا أمرتكم بأمر فأتوا منه ما استطعتم)[٥]، ومن ثم فإن استخدام تقنية التزييف العميق يقع محرمًا لغلبة المفاسد على المصالح والإيجابيات المرجوة منها[٦].

---

(١) صحيح البخاري، كتاب البيوع، باب النجش ومن قال لا يجوز البيع.

(٢) رواه ابن ماجة والدار قطني وغيرهما مسندًا، ورواه مالك في الموطأ.

(٣) د. زكي زكي زيدان: المدخل لدراسة الفقة الإسلامي، التركي للطباعة، ٢٠٠٠، ص ٤١٢.

(٤) أحمد بن على العسقلاني: فتح الباري شرح صحيح البخاري، كتاب الاعتصام بالكتاب والسنة، باب الاقتداء بسنن رسول الله صلي الله عليه وسلم، دار المعرفة للطباعة والنشر، بيروت، لبنان، ج١٣، ص ٢٥١.

د. صالح بن غانم السدلان: القواعد الفقهية الكبرى وما تفرع عنها، دار بلنسة، ١٤١٧هـ، ص٥٠٧.

(٥) صحيح مسلم، كتاب الحج، باب فرض الحج مرة في العمر، ج٤، ص ١٠٢، رقم ١٣٣٧، بنحوه مطولاً حديث مرفوع للنبي -صلى الله عليه وسلم-، سنه قولية، رواه أبي هريرة.

(٦) د. محمد بن عبد العزيز المبارك: قاعدة(درء المفاسد على جلب المصالح) بحث مقدم لمؤتمر القواعد الفقهية على المسائل الطبية، المديرية العامة للشؤون الصحية بالرياض، ١٤٢٨هـ، ص ١٠ .

الشيخ محمد بن أحمد بن محمد: الوجيز في إيضاح قواعد الفقه الكلية، مؤسسة الرسالة العالمية، بيروت، ط٤، ١٩٩٦، ص٢٦٥.

قاعدة (الضرر يزال):

هذه القاعدة أيضًا من القواعد الأصولية في ديننا الحنيف ومن جوامع الأحكام[١]، والضرر يعني الأذى الذي يصيب الإنسان في جسمه أو ماله أو عرضه أو كرامته أو شرفه[٢] ولقد عنت تلك القاعدة بدفع كل ما يترتب عليه أذى للناس، بدءًا من عدم جواز وقوع الأذى، فإذا ما وقع وجب رفعه[٣]، ومن ثم فإذا كان هناك فعل من الأفعال أو تصرف من التصرفات يسبب ضررًا للغير فإنه يجب إزالته[٤]، وبما أن تقنية التزييف العميق تستخدم في التشهير والإضرار بالآخرين فمن ثَمَّ يجب تطبيق هذه القاعدة الفقهية عليها، فالضرر يزال.

قاعدة اعتبار المآلات:

مفاد هذه القاعدة: الاعتداد بما تفضي إليه الأحكام بما يتوافق مع قصد الشارع الحكيم، أي ما يترتب عن الحكم على فعل المكلف من نتائج وغايات [٥]، ومن أقسام اعتبار المآلات ما يكون أداؤه إلى المفسدة كثيرًا لا غالبًا ولا نادرًا، وهذا القسم محرمٌ[٦]، ومآل الفعل هو النتيجة المترتبة على وقوع الفعل، فقصد الشارع أن يكون المآل متوافقًا مع قصد الفاعل، لكن قد يفضي الفعل المشروع إلى مآل لم يقصده[٧]، وبالنظر إلى تقنية التزييف العميق يتبين لنا أن مآلها يؤدي إلى المفسدة حتى ولو لم يقصد فاعله

---

(١) أ. منذرة بنت الحاج سوهيلي: قاعدة الضرر يزال وتطبيقاتها الفقهية، رسالة ماجستير، كلية الشريعة والقانون، جامعة السلطان الشريف على الإسلامي، سلطنة بروناي، ٢٠٢٠، ص ٢.

أ. محمد بن أحمد بن عبد الله: قاعدة الضرر يزال و أثرها في السياسة الجنائية، رسالة ماجستير، كلية العدالة الجنائية، جامعة نايف العربية للعلوم الأمنية، ٢٠١٥، ص ١٤.

(٢) د.زكي زكي زيدان: حق المجني عليه في التعويض عن ضرر النفس في الفقه الإسلامي والقانون الوضعي، دار الكتاب القانوني، ٢٠٠٩، ص٥٤.

(٣) د.شوقي إبراهيم علام: قواعد الفقه الكلية، دراسة نظرية تطبيقية على القواعد الخمس الأمهات وما تفرع عنها من قواعد، دار نهضة مصر، ٢٠١٩، ص٢٢٧.

(٤) د. زكي زكي زيدان: حدود المسئولية عن مضار الجوار، رسالة دكتوراه، جامعة الأزهر، ١٩٩٥، ص٦٧.

(٥) د.وليد بن على حسين: اعتبار مآلات الأفعال وأثرها الفقهي، دار التدمرية، ٢٠٠٩، ص٣٣.

(٦) د.عبد الرحمن بن عبد العزيز السديس: قاعدة (اعتبار المآلات والآثار المترتبة عليها في الفقة الإسلامي والقضايا المعاصرة)، مجلة الشريعة والقانون بالقاهرة، عدد ٣٢، يوليو ٢٠٠٧، ص٤٥.

(٧) د. محمد صلاح حلمي سعد: قاعدة مآلات الأفعال، حجيتها عند الأصوليين، وتطبيقاتها عند الحكيم الترمذي، مجلة الشريعة والقانون بالقاهرة، ع ٤١، إبريل ٢٠٢٣، ص ٢٨٤.

مـا تحقق، ومن ثَـمَّ فإنه بمراعاة قاعـدة اعتبار المآلات يجب القضـاء بتحريمها، ومن هـذه المآلات علـى سبيل المثال: فقدان الثقة في أهل العفـاف، والتشهير بهم، والابتزاز الجنسي لضحايا تقنية التزييف العميق، والتلاعب بالإدلة الجنائية[1].

(١) د.أحمـد مصطفـى معوض محمد محرم: استخدامات الذكاء الاصطناعي - استخدام تقنية التزييف العميق في قذف الغير نموذجًا، دراسة فقهية مقارنة معاصرة، مجلة البحوث الفقهية والقانونية، ع٣٩، أكتوبر ٢٠٢٢، ص ٢٥٤١.

المبحث الثاني

التكييف القانوني لتقنية التزييف العميق

قد خلت التشريعات الأوروبية والعربية من أي نصوص تجريمية حول تقنية التزييف العميق إلا في ولايات أمريكية[١] هم من أدرجوا تجريمًا لتلك التقنية وهم ولاية فرجينيا وولاية كاليفورنيا وولاية نيويورك وولاية جورجينيا[٢]، في حين لم تقدم الحكومة الأمريكية الفيدرالية بعد تشريعًا أو تنظيمًا لمعالجة المشكلة العامة التي تطرحها تقنية التزييف العميق[٣].

ولقد عهدت هذه الولايات إلى التجريم، مع اختلاف جوهرها؛ حيث جرمت فبركة الفيديوهات الإباحية كما جرمت فبركة الفيديوهات للتأثير على العمليات الانتخابية، ويكون بذلك ليس هناك تجريم صريح لشتى أعمال تقنية التزييف العميق.

أولاً- ولاية نيويورك:

في عام ٢٠٢١ تم استحداث نص في قانون الحقوق المدنية في الفصل السادس مادة ٥٢-C [٤] والذي يكمن في تجريم أي محتوي جنسي غير صحيح وتم فبركته، وهي تعني القيام بأداء فعل لم يقوموا به في الواقع[٥].

ثانيًا- ولاية فرجينيا Virginia:

في يوليو ٢٠١٩ صدر قانون لتجريم فبركة الفيديوهات بواسطه تقنية التزييف

---

(١) د. محمود عبد المنعم: مرجع سابق، ص ٣٧٤

(2) Betül Çolak: Legal Issues of Deepfakes- January 19, 2021
https://www.internetjustsociety.org/legal-issues-of-deepfakes
4 States Now have Deepfake Laws (not specific to elections)https://cybercivilrights.org/deep-fake-laws/

(3) Avi Gesser, Megan Bannigan, Christopher Ford, Anna Gressel and Scott Caravello. «Debevoise Discusses Malicious Corporate Deepfakes». Newstex Blogs CLS Blue Sky Blog, February 1, 2023 Wednesday. advance.lexis.com/api/document?collection=news&id=urn:contentItem:67FM-9D11-F03R-N3NT-00000-00&context=1516831. Accessed February 14, 2023.

(4) Private right of action for unlawful dissemination or publication of a sexually explicit depiction of an individual

(5) as a result of digitization, to be giving a performance they did not actually perform or to be performing in a performance that was actually performed by the depicted individual but was subsequently altered to be inviolation of this section.
https://www.nysenate.gov/legislation/laws/CVR/52-C#:~:text=Section%2052%2DC%20Private%20right,explicit%20depiction%20of%20an%20individual
Sales, Jonathan S., and Jessica A. Magaldi. «Deconstructing the Statutory Landscape of'Revenge Porn': An Evaluation of the Elements That Make an Effective Nonconsensual Pornography Statute.» Am. Crim. L. Rev. 57 (2020): p1507

العميق بدون موافقه ذوي الشأن؛ حيث جاءت المادة (٥) من الفصل ٨ [١]: « أي شخص يقوم، بقصد الإكراه أو المضايقة أو التخويف، بنشر أو بيع أي فيديو أو صورة ثابتة تم إنشاؤها بأية وسيلة كانت تصور شخصًا عاريًا تمامًا أو.... حيث يعرف هذا الشخص أنه غير مرخص أو مخول بنشر أو بيع مثل هذه الصور المرئية أو الثابتة، فهو مذنب بارتكاب جنحة من الدرجة الأولى»[٢] ويعتبر استخدام تلك التقنية في إنتاج الفيديوهات المفبركة مجرمًا كوسيلة مستخدمة لإنتاج الفيديوهات المفبركة، وتعد جنحة من الدرجة الأولى.

ثالثًا- ولاية كاليفورنيا California:

نجد أن ولاية كاليفورنيا في ٢٠١٩ أضافت تعديلاً في نص المادة (٣٥) من قانون الإجراءات المدنية[٣] تحذر من استخدام مواد دعائية مزيفة؛ حيث جاء نصها على النحو التالي:

(١) لا يجوز لمرشح لمنصب انتخابي يظهر صوته أو صورته في وسائط صوتية أو مرئية مخادعة ماديًا تم توزيعها بشكل ينتهك هذا القسم أن يطلب أمرًا زجريًا أو غيره من التعويضات المنصفة التي تحظر توزيع الوسائط المرئية

(1) ()FindLaw.com - Virginia Code Title 18.2. Crimes and Offenses Generally § 18.2-386.2. Unlawful dissemination or sale of images of another; penalty - last updated January 01, 2020 | https://codes.findlaw.com/va/title-18-2-crimes-and-offenses-generally/va-code-sect-18-2-386-2.html
Title 18.2. Crimes and Offenses Generally » Chapter 8. Crimes Involving Morals and Decency » Article 5. Obscenity and Related Offenses
https://law.lis.virginia.gov/vacode/18.2-386.2/

(2) A. Any person who, with the intent to coerce, harass, or intimidate, maliciously disseminates or sells any videographic 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 videographic or still image is guilty of a Class 1 misdemeanor. For purposes of this subsection, «another person» includes a person whose image was used in creating, adapting, or modifying a videographic 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.

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

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

(3) An act to amend Section 35 of the Code of Civil Procedure, and to amend Section 20010 of the Elections Code, relating to elections. [Approved by Governor September 29, 2022. Filed with Secretary of State September 29, 2022.]https://legiscan.com/CA/text/AB972/2021

والمسموعـة بشـكل ينتهك هـذا القسم. يحـق لأي إجراء بموجب هـذه الفقرة الأسبقية وفقًا للمادة ٣٥ من قانون الإجراءات المدنية[١].

(٢) يجـوز لمرشـح لمنصب انتخابي يظهـر صوته أو شبهـه في وسائط صوتيـة أو مرئية مخادعـة ماديًا تم توزيعهـا بشكل ينتهك هذا القسم، رفع دعـوى قضائية للحصول علـى تعويضات عامة، أو خاصة ضد الشخص، أو اللجنة، أو الكيان الآخر الذي وزع المـادة المخادعة ماديًـا الوسائط السمعية أو المرئية. يجـوز للمحكمة أيضًا أن تحكم على الطرف السائد أتعاب المحاماة والتكاليف المعقولة. لا يجوز تفسير هذا التقسيم الفرعي للحد من أو منع المدعي من تأمين أو استرداد أي تعويض آخر متاح[٢].

(٣) كمـا هـو مستخـدم فـي هـذا القسـم، يُقصـد بمصطلـح «الوسائـط السمعية أو المرئية المخادعة ماديًا» صورة، أو تسجيل صوتي، أو فيديو لمظهر المرشح، أو حديثه أو سلوكه الذي تم التلاعب به عمدًا بطريقة تجعل كلا الشرطين التاليين استوفيا:

(٤) قـد تبدو الصورة أو تسجيـل الصوت أو الفيديو كاذبـة لأي شخص عاقل أنها أصلية.

(٥) قـد تتسبب الصـورة أو تسجيل الصوت أو الفيديو فـي أن يكون لدى الشخص المعقول فهم أو انطباع مختلف جوهريًا عن المحتوى التعبيري للصورة أو تسجيل الصـوت أو الفيديو عن ذلك الشخص إذا كان الشخص يسمع أو يشاهد ما لم يتم تغييره، النسخة الأصلية من الصورة أو تسجيل الصوت أو الفيديو[٣].

(1) (a) Except as provided in subdivision (b), a person, committee, as defined in Section 82013 of the Government Code, or other entity shall not, within 60 days of an election at which a candidate for elective office will appear on the ballot, distribute, with actual malice, materially deceptive audio or visual media, as defined in subdivision (e), of the candidate with the intent to injure the candidate's reputation or to deceive a voter into voting for or against the candidate

(2) (c) (1) A candidate for elective office whose voice or likeness appears in a materially deceptive audio or visual media distributed in violation of this section may seek injunctive or other equitable relief prohibiting the distribution of audio or visual media in violation of this section. An action under this paragraph shall be entitled to precedence in accordance with Section 35 of the Code of Civil Procedure.

(3) (e) As used in this section, «materially deceptive audio or visual media» means an image or an audio or video recording of a candidate's appearance, speech, or conduct that has been intentionally manipulated in a manner such that both of the following conditions are met:

(1) The image or audio or video recording would falsely appear to a reasonable person to be authentic.

(2) The image or audio or video recording would cause a reasonable person to have a fundamentally different understanding or impression of the expressive content of the image or audio or video recording than that person would have if the person were

Mika Westerlund, «The Emergence of Deepfake Technology: A Review,» Technology Innovation Management Review 9, no. 11 -November 2019: pp39–52

بذلك يكون تعديل المادة (٣٥) من قانون ولاية كاليفورنيا جرم التلاعب في الفيديوهات وإن كان قد قصرها على فيديوهات الدعاية الانتخابية إلاَّ أنه عد بذلك استخدام تلك التقنية وسيلة لارتكاب الجريمة.

رابعًا- ولاية جورجيا Georgia:

نجد أنه تم النص في المادة (١٦) من القانون الجورجي لمكافحة الجريمة على تجريم التلاعب بالفيديوهات؛ حيث جرمت فبركة الفيديوهات الإباحية فيجرم قيام الشخص بإنشاء الفيديوهات المزورة أو الصور الثابتة، ويكون ذلك بهدف الإرسال ومضايقة الغير ويكون لغرض غير مشروع[١].

بل وجعلت مرتكب ذلك مذنبًا بارتكاب جنحة، ويُعاقب بالسجن لمدة لا تقل عن سنة واحدة أو أكثر من خمس سنوات أو غرامة لا تزيد على ١٠٠٠٠٠ دولار أو كليهما[٢].

الجدير بالذكر؛ أن مبادئ القانون الجنائي تؤكد – فيما عدا الحالات النادرة التي يحدد فيها القانون أسلوب الجريمة – أنه لا يهمه الوسيلة التي يتوسل بها الجاني لارتكاب جريمته، لأن الوسائل لدى القانون سواء. فالمشرع لا يجرم الوسيلة المستخدمة، إلاَّ إذا كانت عنصرًا من مكونات الجريمة، فالقانون مثلاً لا يهمه الوسيلة التي يستعين بها الجاني لتنفيذ القتل؛ إذ يستوي في نظره أن يستعمل الجاني يديه عاريتين أو أن يستخدم أداة كعصاة أو مسدس أو خنجر، أم يخنقه بيديه أم يصعقه بتيار كهربائي أو يدفعه من شاهق أو يستخدم لذلك كلبًا مدربًا أو ثعبانًا، أو مجرد تهيئة الوسائل لتفعل فعلها كترك أنابيب الغاز مفتوحة في المنزل أم – وهذا هو الأهم – استخدام أداة إنسانية (إنسانا مفرغاً من الارادة) كالمجنون و الصبي غير المميز، والشخص حسن النية.

(1) A person violates this Code section if he or she, knowing the content of a transmission or post, knowingly and without the consent of the depicted person:
(1) Electronically transmits or posts, in one or more transmissions or posts, a photograph or video which depicts nudity or sexually explicit conduct of an adult, including a falsely created videographic or still image, when the transmission or post is harassment or causes financial loss to the depicted person and serves no legitimate purpose to the depicted person; or
(2) Causes the electronic transmission or posting, in one or more transmissions or posts, of a photograph or video which depicts nudity or sexually explicit conduct of an adult, including a falsely created videographic or still image, when the transmission or post is harassment or causes financial loss to the depicted person and serves no legitimate purpose to the depicted person.
Georgia Code Title 16. Crimes and Offenses § 16-11-90

(2) Any person who violates this Code section shall be guilty of a misdemeanor of a high and aggravated nature; provided, however, that upon a second or subsequent violation of this Code section, he or she shall be guilty of a felony and, upon conviction thereof, shall be punished by imprisonment of not less than one nor more than five years, a fine of not more than $100,000.00, or both
https://codes.findlaw.com/ga/title-16-crimes-and-offenses/ga-code-sect-16-11-90.html

كمـا أنه لا يوجد أي نص فـي التشريعات المقارنة يجرِّم استعمـال تطبيقات الذكاء الاصطناعي حتى ولو كان استخدامها الرئيسي التزييف، والكذب، والتلفيق، ولعل ذلك يُعد دليلاً على أن التجريم يكون تجريم سلوك لا الوسيلة التي تمت بها.

ونجـد أن القانون الجنائي يتطلـب علاقة سببية بين السلـوك والنتيجة الإجرامية، ومـن ثَمَّ فان استخـدام تقنية التزييف العميق تخضـع لإرادة الجاني الحرة، فالتشريع الجنائي المصـري يسلم بحرية الاختيار كأساس لمساءلـة الإنسان جنائيًّا عن جرائمه، لكن هذه الحرية ليست مطلقة وإنما تتأثر بعوامل فردية وبيئية مختلفة، ومن ثَمَّ يختلف مدى المسئولية الجنائية ويتدرج من الانعدام إلى التخفيف وصولاً إلى المسؤولية الكاملة. ومنهـج التشريع المصري في تحديد أساس المسؤولية الجنائية على هذا النحو يتفق مع الاتجاه الإسلامي الذي يقيم مسؤولية الإنسان عن أفعاله على أساس قدرته على اختيار مايأتيـه من أفعال بحرية كاملة، وأن هذه القدرة هي أساس الثواب والعقاب ومن ثم له الحرية الكاملة في استخدامها بشكل مضر للغير أو استخدامها بشكل إيجابي[١]، بناءً عليـه لا عقاب على مستخدم تلـك التطبيقات في الأمور المشروعـة، والتجريم الموجود يكون على الاستخدام غير المشروع [٢]

ومـن ثَمَّ يكـون القانون الجنائي قد اتفق مـع الشريعة الإسلامية فـى أن المُجرَّم هو استخدام تلك التقنية في الإضرار وليس تجريم استخدامها، وهو ما يؤيده الباحث.

(١) د. وليـد سعـد الدين محمـد سعيد: المسئوليـة الجنائية الناشئة عـن تطبيقات الـذكاء الاصطناعي، مجلة العلـوم القانونية والاقتصادية، جامعة عين شمس ع٢، س٣٤، يوليو٢٠٢٢، ص٤١٧.

(٢) د. محمود عبد المنعم: مرجع سابق، ص٢٩.

الفصل الثالث

الصور التجريمية الناشئة عن الاستخدام غير المشروع لتقنية التزييف العميق

تمهيد وتقسيم:

تُعَدُّ الجريمة عدوانًا على المجتمع بأكمله[١]، ومع ذلك لم يعرف قانون العقوبات المصري الجريمة كمعظم القوانين الأخرى، بل اقتصر على بيان أنواعها بحسب درجة جسامتها، فالجريمة في المفهوم القانوني[٢]، تُحصر في السلوك – فعلاً أو امتناعًا –يخالف قاعدة جنائية، ويتقرر لمن يرتكبه جزاء جنائيًا[٣]. الجريمة[٤] هي فعل إيجابي أو سلبي ينتهك قواعد قانون العقوبات[٥].

إن جوهر القانون الجنائي هو حماية المصالح الجوهرية والتي تتمثل في تلك الحالة فى حماية الأفراد من التشهير والإيذاء، وذلك بتجريم الأفعال التي تُسيء إلى الحق أو تُعَرِّض الحق للخطر، عن طريق وضع عقاب رادع في ضوء السياسة الجنائية التي يعتمدها المشرع، وتتسم الصور التجريمية الناشئة عن الاستخدام غير المشروع لتقنية التزييف العميق، بتتابع النشاط كما ذكرنا سلفًا، حيث إن الفيديوهات المزيفة لا تتم إلاَّ بعد عملية رصد وتتبع للصور والفيديوهات المنشورة قبل المجني عليه، ثم العمل على تحريف تلك الفيديوهات والتلاعب بها، واستخدامها في ابتزاز ومساومة المجني عليهم ثم نشرها[٦]. ومن ثم نتناول تلك الجرائم واستعراض المراحل المتعاقبة على النحو التالي:

---

(١) د. سليمان محمد الطماوي: الجريمة التأديبية – دراسة مقارنة، دار الفكر العربي، ١٩٧٥، مصر، ص٧٢.

(2) HENRY CAMPBELL BLACK: BLACK'S LAW DICTIONARY, FOURTH EDITION, THE PUBLISHER'S EDITORIAL STAFF, WEST PUBLISHING CO., 1968, p.445.

(٣) د. سليمان عبد المنعم: أصول علم الإجرام القانوني، دار الجامعة الجديدة للنشر، الإسكندرية، ١٩٩٤، ص٢٣.

(٤) المدلول الجنائي للجريمة هو كل سلوك إنساني يُعاقب عليه قانون العقوبات. فالسلوك لا يعد جريمة إلا إذا قرر له قانون العقوبات جزاء جنائيًا. لكن هذا التعريف للجريمة لا يتضمن عناصرها الأساسية، وإنما هو ينظر إليها من زاوية واحدة، في الأثر المترتب على اقترافها، أي باعتبارها سلوكًا يستوجب العقاب. لذلك فهذا التعريف قاصر عن الاحاطة بحقيقة الجريمة من الناحية الجنائية. وإذا أردنا أن نعرف الجريمة تعريفًا يتضمن عناصرها الأساسية أو أركانها العامة بغض النظر عن نوعها، د. فتوح عبد الله الشاذلي: قانون العقوبات القسم العام، دار المطبوعات الجامعية، ١٩٩٨، ص٦٣-٦٤.

(5) HENRY CAMPBELL BLACK, BLACK'S LAW DICTIONARY, FOURTH EDITION, THE PUBLISHER'S EDITORIAL STAFF, WEST PUBLISHING CO., 1968, p.444.

(٦) د. محمود سلامه عبد المنعم: مرجع سابق، ص٣٨٢.

- المبحث الأول: الصور التجريمية المكوِّنة للمرحلة الأولى.
- المبحث الثاني: الصور التجريمية المكوِّنة للمرحلة الثانية.
- المبحث الثالث: الصور التجريمية المكوِّنة للمرحلة الثالثة.

المبحث الأول
الصور التجريمية المكونة للمرحلة الأولى

تعرف بمرحلة جمع البيانات، ولعلَّ قيام الشخص بالولوج إلى نظام معلوماتي واستخدام البيانات والصور المنشورة به يُعَدُّ أمرًا مجرمًا في حد ذاته ومعاقبًا عليه، وهو ما يشكل جريمة الدخول غير المشروع، وبما أن هذا الولوج دون رضا المسؤول عن البيانات والصور[١] ومن ثم التعرض لها ومعالجتها وصنع المنتج المزيف تعد جريمة في حد ذاتها، ومن ثَمَّ تشكل بداية المرحلة جريمة الدخول غير المشروع لنظام معلوماتي:

أولاً- الأساس القانوني:

جاءت اتفاقية بودابست لمكافحة الجرائم المعلوماتية لعام ٢٠٠١ [٢] في المادة الثانية، التي تنص على أنه: «يجب على كل طرف أن يتبنى الإجراءات التشريعية أو أيه إجراءات آخرى يرى أنها ضرورية من أجل اعتبارها جريمة جنائية وفقًا لقانونه الداخلي ومنها الدخول المتعمد لكل أو لجزء من نظام الحاسب الآلي بدون حق، وبنية إجرامية للحصول على بيانات الحاسب أو آية نية إجرامية آخرى، أو أن ترتكب الجريمة في حاسب آلي يكون متصلاً عن بعد بحاسب آخر»[٣].

في القانون المصري رقم ١٧٥ لسنة ٢٠١٨ نصت المادة (١٤) على أن «يُعاقب بالحبس مدة لا تقل عن ٦ أشهر وبغرامة لا تقل عن ٣٠ ألف جنيه ولا تجاوز ٥٠ ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل إلى موقع[٤] أو حساب خاص[٥]

---

(١) د. حاتم أحمد محمد بطيخ: «تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات (دراسة تحليلية مقارنة)»، مجلة الدراسات القانونية والاقتصادية ع٧، ج١، ٢٠٢١ص ٤١.

(٢) د. خالد حسن أحمد لطفي: مرجع سابق، صـ٧٦

(3) Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.»Convention on Cybercrime- European Treaty Series - No. 185- Budapest, 23.XI.2001https://rm.coe.int/1680081561

د. هلالي عبد اللاه: اتفاقية بودابست لمكافحة جرائم المعلوماتية، دار النهضة العربية، ٢٠٠٧، ص٤٨.

(٤) الموقع: مجال أو مكان افتراضي له عنوان محدد على شبكة معلوماتية، يهدف إلى إتاحة البيانات والمعلومات للعامة أو الخاصة. الجريدة الرسمية – العدد ٣٢ مكرر (ج) في ١٤ أغسطس سنة ٢٠١٨
https://www.cc.gov.eg/legislation_single?id=386006

(٥) الحساب الخاص: مجموعة من المعلومات الخاصة بشخص طبيعي أو اعتباري، تخول له الحق دون غيره الدخول على الخدمات المتاحة أو استخدامها من خلال موقع أو نظام معلوماتي.
الجريدة الرسمية – العدد ٣٢ مكرر (ج) في ١٤ أغسطس سنة ٢٠١٨. https://www.cc.gov.eg/legislation_single?id=386006

أو نظام معلوماتي[١] مستخدمًا حقًا مخولاً له، فتعدى حدود هذا الحق من حيث الزمان أو مستـوى الدخول»[٢]، فقيـام الشخص بالدخول إلى نظـام معلوماتي واستخدام تلك الصـور المنشورة والمعلومات الموجـودة به يُعُّد أمرًا مجرمًا في حـد ذاته ومعاقبًا عليه، وذلك دون رضا المسؤول عن البيانات والصور[٣].

قام المشرع الفرنسي بإصدار قانون «godfrain» في ٥ يناير ١٩٨٨[٤] ثم تم تضمين أحكامه في قانون العقوبات الفرنسي[٥] في المادة٣٢٣-١ بالنص على جريمة الدخول غير المشروع: «يُعاقب على الدخول أو الاستمرار في البقاء في نظام المعلومات المبرمجة أو جزء منه بالحبس لمدة سنتين والغرامة ٦٠٠٠٠ يورو»[٦].

ثانيًا- أركان الجريمة:

١- الركـن المـادي: يحتـل الركن المـادي للجريمـة دورًا هامًا، إذ لا وجـود للجريمة متـى انتفى ركنها المادي. وقد عبر عن تلك الأهميـة العديد من الفقهاء بقولهم إنه من الطبيعي ألا يهتم التشريع العقابي بالنوايا التي لا تخرج إلى الحيز الخارجي، فلا وجود لجريمـة من مجرد النية أو العـزم على ارتكابها مالم تترجم في صـورة مشروع مادى ملموس ذي مظهر خارجي من شأنه إلحاق الضرر بالغير أو على الأقل يهدد بوقوع هذا الضرر[٧].

فالسلـوك الإجرامي في جريمة الدخول غير المشـروع يتحقق بنشاط إيجابي؛ حيث إنهـا من الجرائم الشكليـة التي تعنى بالسلوك الإجرامـي دون اشتراط تحقيق نتيجة؛ حيث يعني تواجد المتهم داخل النظام أو أي من أجزائه سواء طالت تلك المدة أو قصرت

---

(١) مجموعة برامج وأدوات معدة لغرض إدارة ومعالجة البيانات والمعلومات، أو تقديم خدمة معلوماتية.
نص المادة الأولى من القانون ١٧٥ لسنه ٢٠١٨ بشأن مكافحة الجريمة المعلوماتية.
https://www.cc.gov.eg/legislation_single?id=386006

(٢) راجع نصوص القانون علي: https://manshurat.org/node/31487.

(٣) د. أسامه بن غانم: جريمة الدخول غير المشروع إلى النظام المعلوماتي، مجلة دراسات المعلومات، ع١٤، ٢٠١٢، ص١٣.

(٤) د. شريـف نصـر أحمـد: الجوانـب الموضوعية لجرائـم الدخول غير المشـروع إلى الأنظمـة المعلوماتية، مجلة كليـة الشريعة والقانون، ع٣٥، ج٢، ٢٠٢٢، ص٩٠١.

(٥) د. غنام محمد غنام: القانون الجنائي وجرائم تقنية المعلومات، مطبعة جامعة المنصورة، ٢٠٠٨، ص١٣١.

(6) Art. 323-1 Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de (L. no 2004-575 du 21 juin 2004, art. 45-I) «deux ans» d'emprisonnement et de (L. no 2015-912 du 24 juill. 2015, art. 4) «60 000 €» d'amende.

(٧) د. محمود أحمد طه: مبدأ شخصية العقوبات، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ١٩٩٠، صـ١٧٠.

وسواء تحقق له السيطرة على المعلومات من عدمه ولذا فإن كل فعل لا يفضي إلى تخطي حدود النظام لا يعد دخولاً، فمجرد الاطلاع على البيانات والمعلومات لا يعد مجرّما[١].

وقد عبرت القوانين المقارنة بتعبيرات مختلفة منها الدخول غير المشروع، الدخول بدون إذن، الدخول دون حق، ومن ثَمَّ فإن صفة عدم المشروعية تكمن في عدم وجود تصريح للدخول إلى النظام المعلوماتي[٢]، ومن ثم بدون رضا صاحب الحق[٣].

٢- **الركن المعنوي:** جرائم الدخول غير المشروع لجمع البيانات المستخدمة في تقنية التزييف العميق تعد جريمة عمدية؛ حيث يشترط فيها توافر القصد الجنائي العام وهي تعني إرادة الجاني إلى ارتكاب الجريمة مع العلم بأركانها[٤]، مما يعني توافر العلم والإرادة، فيشترط سبق علم الجاني بما يقدم عليه من دخول غير مصرح به إلى النظام المعلوماتي، وأن دخوله غير مصرح به من قبل صاحب الحق[٥]، واتجاه إرادته لذلك، وبما أن تلك الجريمة من الجرائم الشكلية لذا لا تتطلب تحقق نتيجة[٦].

ثالثًا- العقوبة:

نجد أن القانون المصري نص على عقوبة الحبس والغرامة أو بإحدى العقوبتين؛ حيث جاء نص المادة (١٤) علي:«يُعاقب بالحبس مدة لا تقل عن ٦ أشهر وبغرامة لا تقل عن ٣٠ ألف جنيه ولا تجاوز ٥٠ ألف جنيه، أو بإحدى هاتين العقوبتين».

---

(١) د. سومية عكور: الجرائم المعلوماتية وطرق مواجهتها بحث مقدم للملتقى العلمي لكلية العلوم الاستراتيجية، عمان، الأردن، المعنون بـ (الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية، من ٢-٢٠١٤/٩/٤، ص٥.

(٢) د. محمود أحمد طه: المواجهة التشريعية لجرائم الكمبيوتر والإنترنت)، دراسة مقارنة، دار الفكر والقانون، ٢٠١٢، ص٢٣.
د.جميل عبد الباقي الصغير: القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، ١٩٩٢، ص٦٦.

(٣) عرفته المادة الثانية من الاتفاقية الخاصة بحماية الأفراد في مواجهه نظم المعالجة الآلية من قبل المجلس الأوروبي بأنه:«كل شخص طبيعي أو معنوي، أو كل سلطة عامة أو كل مؤسسة أو جهاز يكون لهم سلطة التصرف في نظام الحاسب الآلي التابع إليه وتقرير مضمونه أو محتواه، وكيفية تنظيمه، والهدف منه».
د.مدحت محمد عبد العزيز: الجرائم المعلوماتية الواقعة على النظام المعلوماتي، ٢٠١٥، بدون دار نشر، ص٨١.
د. عمر الفاروق: المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية بدون دار نشر، ١٩٩٥، ص١٢٣.
د.شيماء عبد الغني: الحماية الجنائية للتعاملات الإلكترونية، دار النهضة العربية، ٢٠٠٥، ص٩٩.

(٤) د. هلالي عبد اللاه: شرح قانون العقوبات، القسم العام، دار النهضة العربية، ١٩٨٧، ص٢٢٦.

(٥) د. رأفت جوهري رمضان: المسئولية الجنائية عن أعمال وسائل الإعلام، دار النهضة العربية، ٢٠١١، ص٤١.

(٦) أ. دلخاز صلاح فرحان: الحماية الجنائية الموضوعية للمعلوماتية في القانون العراقي، دراسة مقارنة، رسالة ماجستير، جامعة الإسكندرية، ٢٠١٥، ص١٣٣.

بينمـا جاء قانون العقوبـات الفرنسي في المادة ٣٢٣-١ بالنصـ على عقوبة جريمة الدخـول غير المشروع: «يُعاقب على الدخول أو الاستمرار في البقاء في نظام المعلومات المبرمجة أو جزء منه بالحبس لمدة سنتين والغرامة ٦٠٠٠٠ يورو»[١].

(1) Art. 323-1 Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de (L. no 2004-575 du 21 juin 2004, art. 45-I) «deux ans» d'emprisonnement et de (L. no 2015-912 du 24 juill. 2015, art. 4) «60 000 €» d'amende.

المبحث الثاني

الصور التجريمية المكوّنة للمرحلة الثانية

بعد الانتهاء من مرحلة جمع البيانات والصور الشخصية، ومن ثم تتكون هذه المرحلة والتي تعرف بمرحلة صنع وتزييف الحقيقة والتي تتكون من جريمتين وهما: جريمة معالجة المعطيات الشخصية للغير، وانتهاك الخصوصية دون رضا الشخص، ولذا نقسم هذا المبحث إلى مطلبين اثنين:

- **المطلب الأول: جريمة معالجة المعطيات الشخصية للغير بدون ترخيص.**
- **المطلب الثاني: جريمة انتهاك الخصوصية دون رضا الشخص.**

المطلب الأول

جريمة معالجة المعطيات الشخصية للغير بدون ترخيص

أولاً- الأساس القانوني:

جاءت المادة (٢٦) من القانون المصري رقم ١٧٥لسنه ٢٠١٨ والتي جاء نصها على أن: «يُعاقب 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 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»[(١)].

وجرمها المشرع الفرنسي في قانون العقوبات المادة ٢٢٦-١٦ بأنه: « يُعاقب كل من يقوم بإهمال معالجة البيانات الشخصية دون مراعاة الإجراءات الأولية للقيام بها، والشروط المحددة سلفًا في القانون بالحبس لمدة لا تزيد عن خمس سنوات وبالغرامة المالية والتي يبلغ مقدارها ٣٠٠٠٠ يورو»[(٢)].

---

(١) الجريدة الرسمية – العدد ٣٢ مكرر (ج) في ١٤ أغسطس سنة ٢٠١٨.
https://www.cc.gov.eg/legislation_single?id=386006

(2) Art. 226 >-16 (L. no 2004-801 du 6 août 2004, art. 14) Le fait, y compris par négligence, de procéder ou de faire procéder à des traitements de données à caractère personnel sans qu'aient été respectées les formalités préalables à leur mise en œuvre prévues par la loi est puni de cinq ans d'emprisonnement et de 300 000 € d'amende.
Le livre Ier du code pénal est entré en vigueur le 1er mars 1994 (L. no 92-1336 du 16 déc. 1992, art. 373, mod. par L. no 93-913 du 19 juill. 1993)

ولعـلَّ نصوص التجريم جاءت صريحة بتجريم شتى وسائل الاستخدام غير المشروع لتقنية المعلومات والتي تناولتها المادة الأولى فى القانون المصري رقم ١٧٥ لسنه ٢٠١٨؛ حيـث عرفتهـا بأنها: «أي وسيلة أو مجموعة وسائل مترابطـة أو غير مترابطة تُستخدم لتخزين، واسترجاع، وترتيب، وتنظيم، ومعالجة، وتطوير، وتبادل المعلومات أو البيانات، ويشمـل ذلـك كل ما يرتبط بالوسيلة أو الوسائل المستخدمـة سلكيًا أو لاسلكيًا»[١]، ومن خلال هذا التعريف يكون استخدام تقنية التزييف العميق منشقًا من هذه الوسائل.

والجدير بالذكر أن عملية معالجة البيانات الشخصية للمجني عليهم قد عُرّف في القانون رقم ١٥١ لسنه ٢٠٢٠ والتي تعني «أية عملية إلكترونية أو تقنية لكتـابة البيـانات الشخصيـة، أو تجميعهـا، أو تسجيلها، أو حفظها، أو تخزينهـا، أو دمجها، أو عرضها، أو إرسالهـا، أو استقبالهـا، أو تداولهـا، أو نشرها، أو محوها، أو تغييرهـا، أو تعديلها، أو استرجاعهـا أو تحليلهـا، وذلـك باستخـدام أي وسيـط مـن الوسائـط أو الأجهزة الإلكترونية أو التقنية سواء تم ذلك جزئيًا أو كليًا»[٢]، كما عرفها القانون رقم ١٥٧ لسنه ٢٠١٨ بمكافحـة جرائم تقنية المعلومـات بأنها: «أية عملية إلكترونيـة أو تقنية تتم كليًا أو جزئيًا لكتابة أو تجميع، أو تسجيل، أو حفظ، أو تخزين، أو دمج، أو عرض، أو إرسال، أو استقبـال، أو تـداول، أو نشر، أو محو، أو تغيير، أو تعديـل، أو استرجاع، أو استنباط للبيانات والمعلومات الإلكترونية، وذلك باستخدام أي وسيط من الوسائط أو الحاسبات أو الأجهـزة الأخرى الإلكترونية أو المغناطيسيـة أو الضوئية أو ما يُستحدث من تقنيات أو وسائـط آخـرى»[٣]. كما عرفتها المادة الثانية في اللائحـة العامة الأوروبية للبيانات (GPDR): «أيـة عمليـة أو مجموعة من العمليات التي تتم على بيانات شخصية أو على مجموعه من البيانات الشخصية، سواء كانت أو لم تكن بالوسائل الآلية»[٤].

---

(١) المادة الأولى، الجريدة الرسمية – العدد ٣٢ مكرر (ج) في ١٤ أغسطس سنة ٢٠١٨
https://www.cc.gov.eg/legislation_single?id=386006

(٢) قانـون رقـم ١٥١ لسنـة ٢٠٢٠ بإصـدار قانـون حماية البيانـات الشخصيـة- الجريدة الرسميـة - العدد ٢٨ مكـرر (هـ) - في ١٥ يوليه سنة ٢٠٢٠.
https://www.cc.gov.eg/legislation_single?id=404171

(٣) قانون رقم ١٧٥ لسنة ٢٠١٨، الجريدة الرسمية – العدد ٣٢ مكرر (ج) في ١٤ أغسطس سنة ٢٠١٨.
https://www.cc.gov.eg/legislation_single?id=386006

(4) ‹processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination (…) restriction, erasure or destruction;
Article 4 Definitions-Regulation of the European Parliament and of the Council on the protection of individuals-25 January 2012- p77

ثانيًا - أركان الجريمة:

- **الركن المادي:** تُعد جريمة معالجة البيانات من جرائم السلوك، والتي لا تتطلب تحقيق نتيجة، وإنما يكتفي بأن يصدر عن الجاني السلوك الإجرامي[١]، والذي يتمثل فى استعمال وسيلة تقنية والتي تتمثل هنا فى تقنية التزييف العميق ومعالجة البيانات وربطها بمحتوى مناف للأداب، أو المساس بالشرف، وهو ذو طبيعة شخصية، ترتبط بالجانب المعنوي للمجني عليه[٢]، ومن ثم فهي تشمل صورة صاحب البيانات وصوته[٣]، ويقوم حينئذ الجاني بإجراء تغييرات وتحريف عليها لفعل ما لم تقم بفعله، أو قول ما لم تقله[٤].
- **الركن المعنوي:** هو الإرادة التي توصف بأنها إجرامية وتقترن بالسلوك، هذه الإرادة قد تتخذ صورة القصد الجنائي، فتجعل الجريمة عمدية، وقد تتخذ صورة الخطأ فتجعل الجريمة غير عمدية[٥]، وقد عُرف أيضًا على أنه علم الجاني بالواقعة الإجرامية حال مباشرته للنشاط المادي المحدد له[٦].

وقد عرفت محكمة النقض المصرية الركن المعنوي على أنه: « القصد الجنائي ولم تشترط لقيامهما قصدًا جنائيًا خاصًا، بل يكفى أن يتوافر فيهما القصد الجنائي العام، وهو يتحقق بإدراك الجاني لما يفعل مع علمه بشروطه[٧]».

وبالإمعان في نص المادة (٢٦) من القانون المصري: «كل من تعمد استعمال»، لذا فإن هذه الجريمة من الجرائم العمدية، ولا يتصور وقوع تلك الجريمة عن طريق الخطأ، ومن ثم تتطلب هذه الجريمة القصد الجنائي العام وفقًا للقانون المصري دون القصد الخاص.

---

(١) د.يزيد بوخليط: الجرائم الإلكترونية والوقاية منها، دار الجامعة الجديدة، ٢٠١٩، ص١٩٠.

(٢) د.مدحت رمضان: الحماية الجنائية لشرف واعتبار الشخصيات العامة، دار النهضة، بدون تاريخ نشر، ص١٠، د.أحمد عبد الظاهر: الحماية الجنائية لحق الشخص المعنوي في الشرف والاعتبار، دار النهضة العربية، ٢٠٠٥، ص ١٠٦.

(٣) د.حسام محمد السيد: مرجع سابق، ص ١١٢.

(٤) د.أحمد ذكير: مرجع سابق، ص ٢٢٨١.

(٥) د.فتوح عبدالله الشاذلي: قانون العقوبات، القسم العام، مرجع سابق ص ٦٧.

(٦) د.محمود نجيب حسني: النظرية العامة للقصد الجنائي، دار النهضة العربية، القاهرة، ٢٠٠٦، ص٥٠.

(٧) الطعن رقم ١١١٥٥ لسنة ٨٣ قضائية، الدوائر الجنائية - جلسة ٢٠١٦/٢/٢٥، مكتب فنى (سنة ٦٧ - قاعدة ٣٢ - صفحة ٢٦٧).

إلا أن المشـرع الفرنسي لم يقصرها على التعمـد[١]؛ حيث جاء نص المادة: «بإهمال في المعالجة الإلكترونية»، فمن ثَمَّ تتصور وقوعها عن طريق الخطأ والإهمال[٢].

تعقيـب: يرى الباحـث أن مسلك المشرع الفرنسي بنصه علـى جعل الجريمة معاقبًا عليهـا سواء عن طريق الإهمال أو التعمد يعـد مسلكًا محمودًا، ونناشد المشرع المصري بأن يحذو حذوه.

ثالثًا- العقوبـــة:

يُعاقـب المشرع المصـري وفقًا لنص المادة (٢٦) بالحبس مـدة لا تقل عن سنتين ولا تجـاوز خمس سنوات وبغرامة لا تقل عن مائة ألف جنيـه ولا تجاوز ثلاثمائة ألف جنيه أو بإحـدى هاتـين العقوبتين، بينما يُعاقـب المشرع الفرنسي بالحبس لمـدة لا تزيد على خمس سنوات وبالغرامة المالية والتي يبلغ مقدارها ٣٠٠٠٠ يورو.

المطلب الثاني

جريمة انتهاك الخصوصية دون رضا الشخص

أولاً- الأساس القانونـي:

تنـص المادة (٢٥) مـن قانون مكافحـة جرائـم تقنية المعلومات رقـم١٧٥ لسنـة ٢٠١٨ علـى: «يُعاقـب بالحبس مدة لا تقـل عن ستة أشهر، وبغرامـة لا تقل عن خمسين ألـف جنيـه ولا تجاوز مائة ألف جنيـه، أو بإحدى هاتين العقوبتـين، كل من اعتدى على أي مـن المبادئ أو القيـم الأسرية في المجتمع المصري، أو انتهك حرمة الحياة الخاصة أو أرسـل بكثافـة العديد من الرسائـل الإلكترونية لشخص معـين دون موافقته، أو منح بيانـات شخصية إلى نظام أو موقع إلكتروني لترويـج السلع أو الخدمات دون موافقته، أو نشـر عـن طريق الشبكـة المعلوماتية أو بإحـدى وسائل تقنية المعلومـات معلومات أو أخبـارًا أو صورًا وما في حكمها، تنتهـك خصوصية أي شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أم غير صحيحة».

(١) أ. محمد الشوابكة: جرائم الحاسوب والإنترنت، الجريمة المعلوماتية دار الثقافة للنشر والتوزيع، ٢٠١١، ص ٨٧.

(٢) د. ياسر محمد اللمعي: السياسة الجنائية المعاصرة في حماية خصوصية البيانات الشخصية الإلكترونية، مجلة روح القوانين، كلية الحقوق، جامعة طنطا، أغسطس ٢٠٢١، ص ٢١٤٤.

وجاء قانون العقوبات الفرنسي في المادة (٢٢٦-٢-١) تنص علي: «عندما تتعلق الجرائم المنصوص عليها في المادتين ٢٢٦-١ و٢٢٦-٢ بمحادثات أو صور ذات طبيعة جنسية تم التقاطها في مكان عام أو خاص وتزداد العقوبات إلى الحبس لمدة عامين وغرامة قدرها ٦٠ ألف يورو، في حالة عدم موافقة الشخص على النشر، كل من لفت انتباه الجمهور أو الغير إلى أي تسجيل أو أي مستند يتعلق بمحادثات أو صور ذات طبيعة جنسية تم الحصول عليها بموافقة صريحة أو مفترضة من الشخص أو من تلقاء نفسه، باستخدام أحد الأفعال المنصوص عليها في المادة ٢٢٦-١»[(١)].

ثانيًا- أركان الجريمة:

- **الركن المادي:** يتكون الركن المادي من فعل النشر دون الحاجه إلى تحقق نتيجة، ولعلَّ فعل النشر يتحقق دون النظر إلى عدد من تم إطلاعهم على الصورة ومن ثَمَّ فإن فعل النشر يتحقق ولو كان الأشخاص المطلعون عليها شخصًا واحدًا، وسواء كان النشر بشكل مباشر أو غير مباشر[(٢)]، ومن ثَمَّ يجب أن يتم النشر وفقًا لنص المادة (٢٥) من قانون مكافحة جرائم تقنية المعلومات رقم ١٧٥ لسنة ٢٠١٨ عن طريق النشر على الشبكة المعلوماتية، أو بإحدى وسائل تقنية المعلومات والتي عرفها القانون في المادة الأولى منه بأنه: «أية وسيلة أو مجموعة وسائل مترابطة أو غير مترابطة تُستخدم لتخزين، واسترجاع، وترتيب، وتنظيم، ومعالجة، وتطوير، وتبادل المعلومات أو البيانات، ويشمل ذلك كل ما يرتبط بالوسيلة أو الوسائل المستخدمة سلكيًا أو لاسلكيًا[(٣)]».

الجدير بالذكر أن المادة (٢٥) أشترطت عدم الموافقة على النشر، وجاءت العبارة الأخيرة في المادة ٢٥: «سواء كانت المعلومات صحيحة أم غير صحيحة» ومن ثَمَّ فإن نشر وانتهاك صور الأشخاص الناتجة عن تقنية التزييف العميق يكون محققًا لجريمة انتهاك خصوصية الأشخاص.

(1) Art. 226-2-1 (L. no 2016-1321 du 7 oct. 2016, art. 67) 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.

(٢) د. أحمد ذكير: مرجع سابق، ص ٢٢٧٢.

(٣) الجريدة الرسمية - العدد ٣٢ مكرر (ج) في ١٤ أغسطس سنة ٢٠١٨ https://www.cc.gov.eg/legislation_single?id=386006

بينمـا نجد أن المشـرع الفرنسي جعـل السلـوك الإجرامي يقتصر علـى نشر بدون الموافقـة من قبـل الشخص حتى ولو كان قـد تم جمع هذه البيانـات بموافقة الشخص المعني بالبيانات[١]، ونجد محكمة النقض الفرنسية ترى أن جريمة النشر بدون موافقة الشخـص المعنـي لا يمكـن أن تتعلـق إلاَّ بمستنـد أو تسجيل ناتج في حـد ذاته عن فعل الالتقاط أو التسجيل الذي لم يوافق عليه الشخص»[٢].

- **الركـن المعنوي:** الجديـر بالذكر بأن القصـد المباشر هو توجيه الجـاني إرادته إلى إحـداث نتيجة معينة يريد الوصول إليهـا وهو عالم بصورة يقينية بحدوثها، أو بلزوم حدوثها لأثر حتمي لفعله[٣].

ومن هنا فإن أهم المبادئ الأساسية في التشريع الجنائي الحديث أنه لا جريمة بغير ركن معنوى، فليست الجريمة مجرد فعل ضـار ولكنهـا كذلك إرادة خـالفت نهي الشـارع أو أمـره، ويعبـر عن هذه الإرادة الإجرامية بالركن المعنوي[٤].

تُعـدُّ تلك الجريمة مـن الجرائم العمدية؛ حيث يجب توافر القصد الجنائي العام، فلا يتطلـب تحقق القصـد الخاص، ومن ثم يجـب توافر عنصري العلـم والإرادة، فيجب أن تتجه إرادة الجاني إلى نشر، وأن يكون الجاني عالمًا بأنه ينشر صورة الغير دون رضاه.

- **العقوبة:** نجد أن نص المادة (٢٥) من القانون المصري عاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن خمسين ألف جنيه، ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، بينما نجد المشرع الفرنسي شدد العقاب إلى الحبس لمدة عامين وغرامة قدرها ٦٠ ألف يورو في حالة عدم الموافقة على النشر.

وتطبيقًا لذلك: قضت محكمة طنطا بمعاقبة المتهمين بالسجن ١٥ سنة ونجد أن قرار الإحالة أقر أن المتهمين اعتدوا على حرمة الحياة الخاصة للمجني عليها، ونقلوا صورها بدون رضاها، واستعملوا ونشروا الصور الفوتوغرافية بغير رضا المجني عليه[٥].

(1) Stéphane Detraz: Les nouvelles dispositions réprimant les atteintes à l'intimité sexuelle: faire compliqué quand on peut faire simple (Commentaire de l'article 226-2-1 du code pénal issu de la loi n° 2016-1321 du 7 octobre 2016) Revue de science criminelle et de droit pénal comparé 2016/4 (N° 4), p 750

(2) Cour de cassation, criminelle, Chambre criminelle, 16 mars 2016, 15-82.676, Publié au bulletin

(٣) د. محمـود نجيـب حسنـي: النظرية العامة للقصد الجنائـي، دراسة تأصيليـة مقارنة للركن المعنوي فـي الجرائم العمدية، دار النهضة العربية، ٢٠٠٦، ص ٢٢٤.

(٤) محمد على سويلم: تكييف الواقعة الإجرامية، رسالة دكتوراه، جامعة عين شمس، ١٩٩٩، ص ١٤٦.

(٥) حكم محكمة جنايات طنطا، القضية رقم ٢٠٣٦ كفر الزيات، جلسة ٢٠٢٢/٥/١٠

المبحث الثالث

الصور التجريمية المكونة للمرحلة الثالثة

بعد الانتهاء من مرحلة الجمع ثم مرحلة صنع الفيديوهات والصور نكون قد انتقلنا إلى المرحلة الثالثة وهي مرحلة الغرض، حيث الانتهاء من إعداد الفيديوهات المزيفة والصور والمقاطع التسجيلية ليس هو الغرض النهائي من الاستخدام غير المشروع لتقنية التزييف العميق؛ حيث تكون المرحلة الثالثة وهي الغرض من ذلك التزييف سواء كان بغرض التشويه لسمعة أحد الأشخاص أو تضليل الرأي العام، وسنتناول في هذه المرحلة جريمة التضليل الإعلامي وجريمة الابتزاز الإلكتروني وذلك على النحو التالي:

- **المطلب الأول: جريمة التضليل الإعلامي.**
- **المطلب الثاني: جريمة الابتزاز الإلكتروني.**

المطلب الأول

جريمة التضليل الإعلامي

التضليل الإعلامي يُقصد به كل كذب أو تشويه وإخفاء للحقائق عن الرأي العام[١]، ويكون ذلك بواسطة عرض المنتوج من تقنية التزييف العميق عبر المواقع الإلكترونية أو وسائل التواصل الاجتماعي، بادئ ذي بدء؛ نستعرض المواد المجرَّمة لتلك الجريمة، ونستوضح أركان الجريمة وعقوبتها على النحو التالي:

أولاً- الأساس القانوني للتجريم:

جاءت المادة (٦٥) من القانون المصري (قانون تنظيم مباشرة الحقوق السياسية) «يُعاقب بغرامة لا تقل عن عشرين ألف جنيه ولا تجاوز مائتي ألف جنيه كل من نشر أو أذاع أقوالاً أو أخبارًا كاذبة عن موضوع الانتخاب أو الاستفتاء أو عن سلوك أحد المترشحين أو عن أخلاقه، مع علمه بذلك بقصد التأثير في نتيجة الانتخاب أو

(١) د. ياسر محمد اللمعي: الحماية الجنائية من التضليل الإعلامي أثناء الحملات الانتخابية في ضوء السياسة الجنائية التشريعية، دراسة مقارنة بين التشريعين المصري والقطري، المجلة الدولية للقانون، كلية القانون، جامعة قطر، المجلد٩، ع٣، ٢٠٢٠، ص١٦٨.

الاستفتـاء، فـإذا أذيعت تلك الأقـوال أو الأخبار في وقت لا يستطيـع فيه الناخبون أن يتبينوا الحقيقة ضوعف حدا الغرامة»[١].

مـادة (١٨٨) مـن قانون العقوبـات المصري: «يُعاقـب بالحبس مـدة لا تجاوز سنة وبغرامـة لا تقل عن خمسة آلاف جنيه ولا تزيد على عشرين ألف جنيه أو بإحدى هاتين العقوبتـين كل مـن نشر بسوء قصد بإحـدى الطرق المتقدم ذكرها أخبـارًا، أو بيانات، أو إشاعـات كاذبـة، أو أوراقًا مصطنعة، أو مزورة، أو منسوبـة كذبًا إلى الغير، إذا كان مـن شأن ذلك تكدير السلم العـام أو إثارة الفزع بين الناس أو إلحاق الضرر بالمصلحة العامة»[٢].

ثانيًا- أركان الجريمة:

١- الركـن المـادي: هو النشاط الذي يشكل ماديات الجريمـة، إذ به تظهر الجريمة إلى العـالم الخارجـي، وتتحول من مجرد نية دفينة إلى واقـع محسوس. وللركن المادي عناصره التي يتكون منها وهي: السلوك والنتيجة ورابطة السببية[٣].

فيتحقـق الركـن المـادي للجريمة بتطابـق نشاط الجـاني[٤] لما ورد فـي نص المادة (١٨٨) مـن قانون العقوبات، أو إذا وقـع ذلك التزييف العميق بغرض الإضرار بالحياة السياسية فتنطبق أحكام المادة (٦٥) من قانون تنظيم مباشرة الحقوق السياسية.

أ) السلوك الإجرامي:

يعـد السلوك الإجرامي من أهم عناصر الركن المادي، لأنه يمثل القاسم المشترك بين جميـع أنواع الجرائم، سواء تلك التي يكفي لوقوعها ارتـكاب السلوك الإجرامي فقط أم

(١) الجريدة الرسمية - العدد ٢٣ (تابع) - السنة السابعة والخمسون، ٧ شعبان سنة ١٤٣٥هـ، الموافق ٥ يونيه سنة ٢٠١٤م.
https://www.cc.gov.eg/legislation_single?id=418526

(٢) كان النص القديم في القانون ذاته قبل التعديل:«يُعاقب بالحبس مدة لا تتجاوز ثمانية عشر شهراً وبغرامة لا تقل عن خمسين جنيهـا ولا تزيـد عـن مائتي جنيه أو بإحدي هاتـين العقوبتين « ثم جاء القانـون رقم ٢٩ لسنه ١٩٨٢ معـدلاً ذلك حيث أصبح «يُعاقب بالحبس مدة لا تتجاوز سنة وبغرامة لا تقل عن عشرين جنيهًا أو بإحدي هاتين العقوبتين» إلى أن جاء القانون رقم ٩٣ لسنه ١٩٩٥ معدلا إياها وفقًا لماورد في المتن.
قانون رقم ٥٨ لسنة ١٩٣٧ بإصدار قانون العقوبات وفقاً لآخر تعديل صادر في ٢٠ نوفمبر عام ٢٠٢١.
https://www.cc.gov.eg/legislation_single?id=404680

(٣) د. فتوح عبدالله الشاذلي: قانون العقوبات، القسم العام، دار المطبوعات الجامعية، ١٩٩٨، ص ٦٧.

(٤) د. شريف سيد كامل: الجرائم الصحافية في القانون المصري، دار النهضة العربية، ١٩٩٤، ص١٤٣.

تلك التي يلزم لقيامها ضرورة تحقق نتيجة إجرامية معينة إلى جانب السلوك الإجرامي، وسواء كانت الجريمة تامة أم غير تامة، أي وقفت عند حد الشروع. فلا قيام للركن المادي ولا قيام للجريمة بالتالي إذا تخلف هذا السلوك. فالقاعدة أنه لا جريمة بغير سلوك[١].

ولعلَّ النشاط الإجرامي عن الاستخدام غير المشروع لتقنية التزييف العميق يكون فعل نشر إشاعات وأخبار كاذبة هو جوهر عمل تلك التقنية، ويقصد بها ترديد أقوال غير صحيحة أو نشر فيديوهات أو صور غير مطابقه للواقع حتى ولو لم تتم في العلن[٢].

والأخبار الكاذبة هي الأخبار التي تخالف الواقع كليًا أو جزئيًا؛ حيث يتم القيام باختلاق الخبر برمته أو محرفًا أو مجتزأ [٣]، وتتخذ الأخبار الكاذبة أوجهًا متعددة، ويتم تصنيفها وفقًا للمحتوى المنشورة به على النحو التالي:

- **الهجاء والسخرية:** قد يكون تضمين الهجاء والسخرية في التضليل.
- **الأخبار المضللة:** حيث تحمل هذه الأخبار معلومات حقيقية تم توظيفها في سياق خطأ، وغالبًا ما تكون تلك الاقتباسات تم انتقاؤها بدقة.
- **الربط الخاطئ:** حيث تكون أخبارًا ذات صلة تحمل عناوين ليس لها علاقة بالموضوع، أي أن العناوين المنشورة أو المذاعة التي تم بثها عبر أي وسيلة كان محتواها حقيقيًا[٤].

بل ليس ذلك فحسب، بل إن السلوك الإجرامي يشمل كل فعل أو امتناع عن فعل يتحقق فيه العلانية[٥]، وقد يقتصر دور الجاني في مجرد ترديد ما سمعه ورآه إلى الآخرين[٦]، وفي ظل التطور التكنولوجي الهائل يكون العمل على نشرها وعرضها للجمهور على صفحات السوشيال ميديا ونشرها بشكل واسع؛ حينئذ يكون الشخص

(١) د. فتوح عبدالله الشاذلي: قانون العقوبات، القسم العام، مرجع سابق، ص ٣٩٦.

(٢) د.طارق سرور: جرائم النشر والإعلام، دار النهضة العربية، ٢٠٠٤، ص ٤٢٢.

(٣) د.محمد هشام أبو الفتوح: الشائعات في قانون العقوبات المصري والقوانين أخرى، دار النهضة العربية، ١٩٩٥، ص٧٣.

(٤) د.نبيل لحمر: الأخبار الكاذبة عبر شبكات التواصل الاجتماعي وآثارها على اتجاهات الرأي العام، دراسة في المفهوم والعلاقة، مجلة الباحث للدراسات الأكاديمية، المجلد ٧، ع ٢، ٢٠٢٠، ص ٥٨٤.

(٥) د.أنور محمد السيد خلف: الحماية الجنائية للتصويت في الانتخابات، دراسة مقارنة، رسالة دكتوراه، جامعة طنطا، ٢٠٢٠، ص ٢١١.

(٦) د.حسام الدين محمد أحمد: الحماية الجنائية للمبادئ الحاكمة للانتخابات السياسية في مراحلها المختلفة، دار النهضة العربية، ٢٠٠٢، ص ١٤٤.

مرتكبًا لجريمة نشر إشاعات كاذبه؛ حيث يجب أن يستوثق الناشر من صحة تلك الفيديوهات والصور المفبركة قبل عرضها والتوسع في نشرها، وذلك وفقًا لنص المادة ١٩٧ من قانون العقوبات المصري والتي جاء نصها على أن : «لا يقبل من أحد، للإفلات من المسئولية الجنائية مما نص عليه في المواد السابقة، أن يتخذ لنفسه مبررًا أو أن يقيم لها عذرًا من أن الكتابات أو الرسوم أو الصور أو الصور الشمسية أو الرموز أو طرق التمثيل الأخرى إنما نقلت أو ترجمت عن نشرات صدرت في مصر أو في الخارج أو أنها لم تزد على ترديد إشاعات أو روايات عن الغير».

ب) النتيجة الإجرامية:

يتعين أن يكون نشر هذه الفيديوهات أو الصور بغرض التأثير على النظام العام سواء بتضليل الأشخاص العامة أو محاولة تشويه الغير.

- **الركن المعنوي:** جاءت المادة (١٨٨) من قانون العقوبات المصري محددًا للفظ «كل من نشر بسوء قصد» أي أن العلم يجب أن ينصرف إلى مضمون تلك الفيديوهات والصور وإلى كونها غير حقيقية، وهو ما أكدته محكمة النقض المصرية؛ حيث أوردت في حكمها «أنه يجب لتطبيق المادة ١٨٨ من قانون العقوبات الخاصة بنشر الأخبار الكاذبة مع سوء القصد أن يكون الخبر كاذبًا وأن يكون ناشره على علم بهذا الكذب ومتعمدًا لنشر ما هو مكذوب»[١].

ولقد ثار خلاف فقهي حول نوع القصد الجنائي المطلوب في هذه الجريمة، فيري جانب من الفقه أن الناشر كان يعلم أن هذه الصور والفيديوهات مزورة ومزيفة ويجب أن تكون نية الناشر قد اتجهت نحو إحداث هذه النتائج[٢]، ومن ثم يكون المرجو هو القصد الجنائي الخاص، بينما يرى جانب آخر أن عبارة سوء النية أو سوء القصد كان لغرض إلقاء عبء الإثبات على النيابة العامة في معنى علم الناشر بكذب الخبر، ولا يُقصد به قصد جنائي خاص[٣].

---

(١) الطعن رقم ٤٥١ لسنة ٢٢ق، نقض ٢٠ مايو ١٩٥٢، مجموعة الربع قرن، ج٢، ص١٠٦١، الطعن رقم ٩٨٤٨ لسنه ٨٧ق، جلسة ٢ فبراير ٢٠١٩، للإطلاع على صورة الحكم: https://elhak.org/wp-content/uploads/2020/02/%D9%85%D8%AD%D9%83%D9%85%D8%A9-%D8%A7%D9%84%D9%86%D9%82%D8%B6-%D8%B7%D8%B9%D9%86-%D8%B1%D9%82%D9%85-9848.pdf.

(٢) د. خالد رمضان عبد العال: المسئولية الجنائية عن جرائم الصحافة، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة حلوان، ٢٠٠٢، ص ٣٣٥.

(٣) د. وفاء محمد أبو المعاطي صقر: المسئولية الجنائية عن بث الشائعات عبر مواقع التواصل الاجتماعي، مجلة روح القوانين،

- **العقوبة:** يُعاقب بالحبس مدة لا تجاوز سنة وبغرامة لا تقل عن خمسة آلاف جنيه ولا تزيد على عشرين ألف جنيه أو بإحدى هاتين العقوبتين.

المطلب الثاني

جريمة الابتزاز الإلكتروني

الابتزاز من الجرائم الأخلاقية وهي كجريمة تشكل في حد ذاتها العديد من الجرائم الأخرى كالتهديد والترويع[١] والتشهير وإشاعة الفاحشة[٢]، وعرفت بأنها التهديد بإيقاع الأضرار سواء النفسية أو الجسدية على المجني عليه[٣]، لذا من الممكن تعريفه بلفظ الاغتصاب الإلكتروني؛ حيث عرف بأنه: «أخذ الشيء بجفاء من غير رضى صاحبه»[٤] وهو بالأحرى يعد مكوناً لفكرة اغتصاب الشيء من صاحبه سواء كان ذلك- مادياً أو معنوياً-، وعرفت بأنها:«محاولة الحصول على شيء من شخص ما عنوة».

ولقد عرفه المشرع الفرنسي في المادة ٣١٢-١ من قانون العقوبات بأنه:«فعل الحصول على الشيء بالعنف أو التهديد بالعنف أو الإكراه للتوقيع أو التعهد أو التخلي أو الكشف عن سر أو تحويل أموال»[٥].

الجدير بالذكر أن جريمة الابتزاز ليست بالظاهرة المستحدثة بل هي قديمة فلقد ذكر الله سبحانه وتعالى في القرآن الكريم عن امرأة العزيز أنها راودت سيدنا يوسف عليه السلام وهددته بأنه سيودع في السجن في حال عدم قيامه بما تطلب، وذلك لقول

ع٩٣، يناير ٢٠٢١، ص ٩٨.

(١) التهديد بالقتل أو بالإيذاء الذي يقع على النفس، وكذلك ترويع الآمنين في أرواحهم أو أعراضهم أو أموالهم تعتبر من الجرائم المحرمة التي تقع على الفرد والمجتمع في آن واحد.

(٢) الابتزاز فيه تهديد بالتشهير بالضحية بما يمس شرفها وعرضها، وهذا يتنافى مع الشريعة الإسلامية التي تحث على الستر كما في حديث يعلى بن أُمية قَالَ -صَلَّى اللهُ عَلَيْهِ وَسَلَّمَ-: «إِنَّ اللَّهَ عَزَّ وَجَلَّ حَيِيٌّ سِتِّيرٌ يُحِبُّ الْحَيَاءَ وَالسَّتْرَ».

(٣) أ.ريم أحمد محماس الدوسري: القذف والابتزاز الإلكتروني بين الشريعة والقانون الكويتي، المجلة القانونية، كلية الحقوق، جامعة القاهره، ع ٤ مج١٦، مايو ٢٠٢٣، ص ١٠٢٥.

(٤) د.هيفاء محمد عيد: القواعد الفقهية المتعلقة بجريمة الإبتزاز الإلكتروني، دراسة فقهية قانونية، مجلة الأستاذ للعلوم الإنسانية والاجتماعية، مج٦١، ع٤، ٢٠٢٢، ص ٣٣٢.

(5) 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.

اللّه تعالى: ﴿قَالَتْ فَذَلِكُنَّ الَّذِي لُمْتُنَّنِي فِيهِ وَلَقَدْ رَاوَدْتُهُ عَنْ نَفْسِهِ فَاسْتَعْصَمَ وَلَئِنْ لَمْ يَفْعَلْ مَا آمُرُهُ لَيُسْجَنَنَّ وَلَيَكُونًا مِنَ الصَّاغِرِينَ﴾[1] ومن الواضح من هذه الآية الكريمة أن امرأة العزيز لجأت إلى ابتزاز سيدنا يوسف عليه السلام لتحقيق مرادها وهو تهديد الشخص وابتزازه؛ ولذا نؤكد أن جريمة الابتزاز ليست بالحديثة ولكن ارتباطها بالإلكترونيات أضحى الأمر وكأنه مستحدث.

أولاً- الأساس القانوني:

لقد حرص الإسلام على احترام الخصوصية، وتحريم أي انتهاك لها؛ قال تعالى «وَلا تَجَسَّسُوا» [2]، وكذلك حرم الاعتداء على النفس والمال والعرض؛ قال تعالى (وَلَا تَعْتَدُوا إِنَّ اللَّهَ لَا يُحِبُّ الْمُعْتَدِينَ)[3].

وعَنْ ابْنِ عُمَرَ (رضي اللّه عنهما) قَالَ: صَعِدَ رَسُولُ اللَّهِ -صَلَّى اللَّهُ عَلَيْهِ وَسَلَّمَ- الْمِنْبَرَ فَنَادَى بِصَوْتٍ رَفِيعٍ، فَقَالَ: «يَا مَعْشَرَ مَنْ أَسْلَمَ بِلِسَانِهِ وَلَمْ يُفْضِ الإِيمَانُ إِلَى قَلْبِهِ، لَا تُؤْذُوا الْمُسْلِمِينَ وَلَا تُعَيِّرُوهُمْ وَلَا تَتَّبِعُوا عَوْرَاتِهِمْ، فَإِنَّهُ مَنْ تَتَبَّعَ عَوْرَةَ أَخِيهِ الْمُسْلِمِ تَتَبَّعَ اللَّهُ عَوْرَتَهُ، وَمَنْ تَتَبَّعَ اللَّهُ عَوْرَتَهُ يَفْضَحْهُ وَلَوْ فِي جَوْفِ رَحْلِهِ» [4]، وهذا نهي صريح عن تتبع عورات الناس، وتصيّد أخطائهم، ومن ثمّ ابتزازهم. ولقد أصبح حال عالمنا العربي اليوم لا يرثى له، من كثرة ما انتهكت خصوصيات، واحترقت أرواح، خوفًا من الفضيحة، فهذه الجريمة البشعة، قد هدمت الكثير من البيوت، ودمرت الكثير من الفتيات.

ونجد التشريع المصري جرّمها في قانون العقوبات المصري؛ حيث جاءت المادة٣٠٩ مكررًا (أ) تنص على أن: «يُعاقب بالحبس كل من أذاع أو سهل إذاعة أو استعمل ولو في غير علانية تسجيلًا أو مستندًا متحصلًا عليه بإحدى الطرق المبينة بالمادة السابقة أو كان بغير رضاء صاحب الشأن، ويُعاقب بالسجن مدة لا تزيد على خمس سنوات كل من هدد بإفشاء أمر من الأمور التي تمَّ التحصل عليها بإحدى الطرق المشار إليها لحمل

(١) سورة يوسف: ٣٢.

(٢) سورة الحجرات: من الآية ١٢.

(٣) سورة البقرة: من الآية ١٩٠.

(٤) سنن الترمذي: أبواب البر والصلة عن رسول الله صلى الله عليه وسلم- باب ما جاء في تعظيم المؤمن، ج٤/٣٧٨، حديث رقم٢٠٣٢، قال الترمذي: حديث حسن غريب.

شخص على القيام بعمل أو الامتناع عنه. ويُعاقب بالسجن الموظف العام الذي يرتكب أحد الأفعال المبينة بهذه المادة اعتمادًا على سلطة وظيفته. ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة أو تحصل عنها، كما يحكم بمحو التسجيلات المتحصلة عن الجريمة أو إعدامها[١]».

ومن الجدير بالذكر أن نص المادة (٣٢٧) من ذات القانون نصت على أنه: «كل من هدد غيره كتابةً بارتكاب جريمة ضد النفس أو المال معاقب عليها بالقتل أو السجن المؤبد أو المشدد أو بإفشاء أمور مُخدشة بالشرف، وكان التهديد مصحوبًا بطلب أو بتكليف بأمر يُعاقب بالسجن. ويُعاقب بالحبس إذا لم يكن التهديد مصحوبًا بطلب أو بتكليف بأمر.

وكل من هدد غيره شفهيًّا بواسطة شخص آخر بمثل ما ذكر يُعاقب بالحبس مدة لا تزيد على سنتين أو بغرامة لا تزيد على خمسمائة جنيه سواء أكان التهديد مصحوبًا بتكليف بأمر أم لا. وكل تهديد سواء أكان كتابة أم شفهيًّا بواسطة شخص آخر بارتكاب جريمة لا تبلغ الجسامة المتقدمة يُعاقب عليه بالحبس مدة لا تزيد على ستة أشهر أو بغرامة لا تزيد على مائتي جنيه»[٢].

وعلى ذات المنوال جرَّم المشرع الفرنسي هو الآخر هذه الأفعال؛ حيث جاءت المادة (٣١٢-١٠) من قانون العقوبات الفرنسي تنصُّ على أن: «الحصول عن طريق التهديد بكشف أو ادعاء وقائع من شأنها أن تضرَّ بالسمعة والشرف يُعاقب على ذلك الابتزاز بالسجن خمس سنوات وغرامة ٧٥٠٠٠يورو»[٣].

ثانيًا- أركان الجريمة:

- **الركن المادي:** يتخذ السلوك الإجرامي في جريمة الابتزاز صورة التهديد ويجب أن يكون هذا التهديد مقترنًا بطلب؛ حيث إنه إن لم يقترن بطلب لا يعد ابتزازًا[٤].

(1) نص المادة 309: https://masaar.net/egypt_laws/%D8%A7%D9%84%D9%85%D8%A7%D8%AF%D8%A9-309-%D9%85%D9%83%D8%B1%D8%B1-%D8%A3/

(2) https://manshurat.org/node/14677

(3) ‹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 € d'amende

(٤) د. تامر صالح: الابتزاز الإلكتروني، دراسة تحليلية مقارنة، ص ٥٧٥.

والجديـر بالذكـر أنه يجب أن يكـون ذلك التهديـد جديًا، وليس علـى سبيل المزاح فلقـد أكدت محكمـة النقض على ذلـك في حكمها؛ حيـث نصت علـى: «إذا كان يبين مـن الاطلاع على خطـاب التهديد كما أورده قرار غرفة الاتهـام المطعون فيه أن ظاهر عباراتـه تحمـل طابع الجد لأن الدافع إلى توجيهه كما ورد به هو النزاع على أطيان وإن عبـارات التهديد التى تكـررت فى موضع من الخطاب المذكور صريحة فى مدلولها دالة بذاتها على التهديد بالقتل المصحوب بطلب، مما من شأنه أن يمس بطمأنينته من توجه إليـه وتتحقق به أركان جريمة التهديد بالكتابة، المصحـوب بطلب المنصوص عليها فى المـادة (٢٨٤) فقـرة أولى من قانون العقوبات، فإن القـرار المطعون فيه إذ قضى بعدم وجـود وجه لإقامة الدعوى العمومية لمجرد القول بـأن عبارات التهديد غير جدية وأنها قرينـة بأن محمل لعب الأطفـال وعبثهم لا محل الجد مما لا تتحقـق به جريمة عمدية دون أن تبين غرفة الاتهام وجه استنادها فى العدول عن ظاهر مدلول العبارات موضوع التهمة إلى القول بعدم جديتها. هذا القصور يكون منطويًا على القصور مما لا تستبين معـه محكمة النقض إن كانت نصوصـ القانون قد طبقت على الواقعة كما هى مثبتة به تطبيقًا صحيحًا أم لا. ولذا فان هذا القرار يكون معيبًا متعينًا نقضه»[١].

ويستـوي التهديد إذا وقع مباشرًا أي تم تهديد الشخـص بشكل مباشر أو تم إرسال بعض عبـارات التهديـد مع غيره، وهو مـا أكد عليـه قضاء محكمة النقض المصرية: «لمـا كان يكفـي للعقاب بموجب الفقـرة الأولى من المادة ٣٢٧ المشـار إليها – من قانون العقوبات – أن يكون الجاني قد بعث رسالة التهديد لتصل إلى علم المراد تهديده، سواء أرسلهـا إليه فتلقاهـا مباشرة، أم بعث بها إلى شخص آخر فتلقاها هذا الآخر ثم بلغها إياه أو لم يبلغها، ثم إنه لا يشترط أن يكون الجاني الذي يختار هذا الطريق الأخير في توجيـه نذيره قد قصـد أن يقوم من أرسلـت إليه بتبليغها إلى المعني بهـا، بل يكفي أن يثبت في حقه أنه لا يجهل أن الطريق الذي اختاره يتوقع معه حتمًا أن المرسل إليه بحكم وظيفته أو بسبب علاقته أو صلته بالشخص المقصود بالتهديد سيبلغه الرسالة، ومن ثم فإن ما يُثار في هذا الصدد يكون غير سديد»[٢].

- **الركن المعنوي:** ولا تختلف جريمة الابتزاز عن سابقيها في الركن المعنوي ووجوب

(١) الطعن رقم ٢٠٩٣ لسنة ٢٣ بتاريخ: ١٨/٠٥/١٩٥٤.

(٢) الطعن رقم ٢٢٨٣٠ لسنة ٨٨ بتاريخ: ١١/٠٩/٢٠٢١

توافر العلم والإرادة، فنجد محكمة النقض المصرية تؤكد في حكمها على القصد الجنائي بقولها: «لما كان القصد الجنائي في جريمة التهديد المصحوب بطلب يتوافر متى ثبت لمحكمة الموضوع أن الجاني ارتكب التهديد وهو يدرك أثره من حيث إيقاع الرعب في نفس المجني عليه، مما قد يكرهه على أداء ما هو مطلوب منه وهو في الدعوى المطروحة إخلاء العين التي يشغلها والتي يستأجرها من الطاعن – وقد أثبت الحكم المطعون فيه على نحو ما سلف بيانه ذلك، فإن ما يثيره الطاعن في هذا الشأن يكون على غير أساس»[1].

ثالثًا- العقوبة:

فرق المشرع المصري في أحكامه إذا كان المتحصل عليه من المعلومات قد تم بحكم الوظيفه فيُعاقب الموظف العام بالسجن مدة لا تزيد على خمس سنوات، وذلك وفقًا لما ورد في نص المادة ٣٠٩ مكررًا (أ) من قانون العقوبات المصري.

بينما إذا كان ذلك الشخص المُهدد من غير الموظفين العموميين، وكان تهديده مصحوبًا بطلب أو بتكليف بأمر يُعاقب بالسجن. أمَّا في حالة إذا لم يكن التهديد مصحوبًا بطلب أو بتكليف بأمر عوقب بالحبس، وتأكيدًا على ذلك نطالع حكم محكمة النقض المصرية والذي جاء نصه على: «لما كان الحكم المطعون فيه بعد أن بين واقعة الدعوى بما تتوافر به العناصر القانونية لجرائم هتك عرض طفلة والتقاط صور لها في مكان خاص ونشرها وتهديدها كتابة بإفشاء أمور خادشة للحياء لحملها على القيام بعمل التي دان المطعون ضده بها، وأورد على ثبوتها في حقه أدلة سائغة، انتهى إلى عقابه طبقًا للمواد ٢٦٨، ٣٠٩ مكررًا / ١ بند ب، ٣٠٩ مكرر أ / ١، ٢، ٣٢٦، ٣٢٧ / ١ من قانون العقوبات، والمواد ٢ / ١، ٩٥ / ١ – ١١، ١١٦ مكررًا، ١٢٢ / ٢ من القانون رقم ١٢ لسنة ١٩٩٦ المعدل بالقانون رقم ١٢٦ لسنة ٢٠٠٨، ثم أوقع عليه عقوبة الحبس مع الشغل لمدة سنتين وذلك بالتطبيق للمادتين ١٧، ٣٢ من قانون العقوبات. لما كان ذلك، وكان البند الأخير من المادة (٣٠٩) مكررًا من قانون العقوبات التي دين المطعون ضده بها ينص على أنه: ويحكم في جميع الأحوال بمصادرة الأجهزة وغيرها مما يكون قد استخدم في الجريمة أو تحصل عنها، كما يحكم بمحو التسجيلات المتحصلة عنها

(١) الطعن رقم ١٧٨٨١ لسنة ٨٤ جلسة ٢٠١٥/١٠/٢٠

أو إعدامها. ولما كانت عقوبة محو التسجيلات المتحصلة عن الجريمة هي عقوبة تكميلية واجـب الحكـم بها، وكان الأصـل أن العقوبة الأصليـة المقررة لأشـد الجرائم المرتبطة ارتباطًـا لا يقبـل التجزئة تجب العقوبـة الأصلية لما عداها من جرائـم مرتبطة بها، إلا أن هـذا الوجـوب لا يمتد إلى العقوبـات التكميلية المنصوص عليها فـي هذه الجرائم، ولمـا كانت عقوبة محـو التسجيـلات المتحصلة عن الجريمـة هي عقوبـة نوعية تراعى فيهـا طبيعة الجريمة، ولذلك يجب توقيعها مهما تكن العقوبة المقررة لما ترتبط به هذه الجريمة من جرائم آخرى والحكم بها مع عقوبة الجريمة الأشد. لما كان ما تقدم، فإن الحكـم المطعون فيه؛ إذ أغفل القضاء بمحو التسجيلات المتحصلة عن الجريمة إعمالا لنص البند الأخير من المادة ٣٠٩ مكررًا من القانون المشار إليه يكون قد خالف القانون، بمـا يتعين معـه تصحيحه بإضافة عقوبة محو التسجيـلات المتحصلة عن الجريمة إلى العقوبة المقضي بها»[١].

كما عاقب المشرع المصري كل من هدد غيره شفهيًّا بواسطة شخص آخر وكل تهديد سـواء أكان كتابـة أم شفهيًّـا بواسطـة شخص آخـر بارتكاب جريمة لا تبلـغ الجسامة المتقدمـة يُعاقب عليه بالحبس مدة لا تزيد على ستة أشهر أو بغرامة لا تزيد على مائتي جنيـه، ويستوى أن تكون هـذه الكتابة إلكترونيًّا عن طريق وسائـل التواصل الاجتماعي أو بالطرق التقليدية وهو ما أكدت عليه محكمه النقض المصرية في حكمها والذي نص علـى: «لما كانت جناية التهديـد المنصوص عليها في الفقـرة الأولى من المادة ٣٢٧ من قانون العقوبات تتوافر إذا وقع التهديد كتابة بارتكاب جريمة ضد النفس أو المال، وكان التهديـد مصحوبـاً بطلب أو تكليف بأمـر، وكان الحكم قـد أورد بأسبابه قيام الطاعن بتهديـد المجني عليهما عبر مواقع التواصل الاجتماعـي، وتمكن من خداعهما وتحصل منهمـا على صور ومقاطع مرئية في أوضاع مخلـة بالحياء وهددهما بنشرها، وإذ كان مصطلـح الكتابـة قد ورد في المادة ٣٢٧ سالفة الذكر على سبيل البيان في صيغة عامة لتشمـل كافة وسائل الكتابـة المختلفة سواء كانت بالطرق التقليديـة أو بإحدى الوسائل الإلكترونية الحديثة، فإذا أثبت الحكم على الطاعن إرساله عبارات التهديد عن طريق الوسائـط الإلكترونيـة الحديثة – وهـي لوحة المفاتيح – بقصد إيقـاع الخوف في نفس المجنـي عليهما لحملهما على أداء ما هو مطلـوب، فإنه يكون قد استظهر أركان جريمة

(١) الطعن رقم ٣٢٢٤ لسنة ٩٠ بتاريخ: ٠٥/٠٩/٢٠٢١

التهديد كما هي معرفة به في القانون، ويضحى منعى الطاعن في هذا الشأن على غير أساس[1]».

وحسناً ما فعله المشرع المصري بالتجريم، وإن كنَّا نرى تشديد العقوبة؛ نظرًا لكون الابتزاز الناتج عن تقنية التزييف العميق يكون نابعًا من نية إجرامية وشخصية خطرة.

(١) الطعن رقم ٢٢٦٢٠ لسنة ٨٨ بتاريخ: ٠٩/٠٧/٢٠٢٠

الفصل الرابع

المسئولية الجنائية عن الاستخدام غير المشروع لتقنية التزييف العميق

تمهيد وتقسيم:

إن التشريعات الجنائية الحديثة تجمع على اعتبار الإنسان الحي متحملاً للمسؤولية الجنائية إذا تحقـق مناطها وهو الإدراك وحرية الاختيار[١]، فالإنسان هو الذي يرتكب الجريمـة، ولا يتصور أن يرتكبها الحيوان أو يساهـم فيها مع الإنسان؛ لأن الحيوان قد يكـون أداة تستعمل في ارتـكاب الجريمة، فيسأل عن الجريمـة الإنسان وحده[٢]، لكن الإنســان قـد يرتكب الجريمـة ولا يُسأل عنهـا إذا تخلف مناط المسؤوليـة، أي الإدراك وحرية الاختيـار، فالصغير والمجنون والمكـره والمضطر يرتكبون الأفعـال التي يجرمها التشريـع الجنائي، لكنهـم لا يُسألون جنائيًّا عن هذه الأفعـال لانتفاء التمييز والإدراك وحريـة الاختيار لديهـم[٣]، ويستنبط ذلك مـن نص المادة (٦٢) مـن قانون العقوبات ٢٠٠٩، ونصت على أنه «لا يُسأل جنائيًّا الشخص الذي يعاني وقت ارتكاب الجريمة من اضطـراب نفســي أو عقلي أفقده الإدراك أو الاختيـار، أو الذي يعاني من غيبوبة ناشئة عـن عقاقـير مخدرة أياً كان نوعها إذا أخذها قهرًا عنه أو على غير علم منه بها» ويعبر عـن ذلك بمبدأ أساسي في القوانين الحديثة هو مبـدأ شخصية المسؤولية الجنائية[٤] الذي أقرته الشريعة الإسلامية في أصل التشريع الإسلامي[٥].

---

(١) د. عوض محمد: قانون العقوبات – القسم العام، دار المطبوعات الجامعية، الإسكندرية، ١٩٩٨، ص٤١٧.

(٢) د. محمد راشد مانع العجمي: المسئولية الجنائية للشخص المعنوي، مجلة البحوث الفقهية والقانونية، ع٣٧، إبريل ٢٠٢٢، ص ١٧٩٠.
د.سامح السيد جاد: شرح قانون العقوبات، القسم العام، دون دار نشر، ٢٠٠٥، ص ٣٤٣.

(٣) د. فتـوح عبد الله الشاذلي: المسئولية الجنائية، دار المطبوعات الجامعية، الاسكندرية، ٢٠٠٦، ص ٢٣.

(٤) يتفرع عن هذا المبدأ، مبدأ هام وهو شخصية العقوبة وهو ما يعني أنه لا يتحمل وزر العقوبة إلاَّ من تقررت مسئوليته، د. أحمد فتحـي سـرور: الوسيط في قانون العقوبـات، القسم العام، الطبعة السادسة، نادي القضـاة، ٢٠١٥، ص٧١٨، د. أحمد فتحي سرور: القانون الجنائي الدستوري، دار الشروق ٢٠٠٢، ص ١٩٧.
A.Batteur: De la protection du corps à la protection de l'être humain, petites affiches, 14 décembre 1994, P.29.
L.Becker: Les limites du concept d'être humain, Cahier STS (Science – Technologie- Société(, n°11, Éthique et biologie, Ed, du Commission nationale de déontologie de la sécurité, 1986, P.139.
D.Bourg: Sujet-Personne-individu-Droits, 1991, n°13, Biologie, personne et droit, P.U.F, 1991, P.87.

(٥) د. علـى عبـد القـــادر القهوجـي، د. فتـوح عبـد الله الشاذلي: شرح قانـون العقوبات القسم العام، الكتـاب الثاني المسئولية والجزاء، بدون دار نشر، ٢٠٠٤، ص ٢٤.

والجدير بالذكر أن الجريمة الواقعة لم تكن وليدة نشاط شخص واحد ولا ثمرة لإرادته وحده، وإنما أسهم في إبرازها إلى حيز الوجود عدة أشخاص، كان لكل منهم دور يؤديه[١]، هذا الدور يتنوع في طبيعته ويتفاوت في أهميته في تحقيق الجريمة على نحو يثير العديد من المشاكل القانونية في تحديد أثر هذا التنوع والتفاوت في أحكام القانون فقد يكون دور المسهم هو الدور الرئيسي في الجريمة[٢]، فتكون مساهمته في إحداثها مساهمة أصلية ويسمى هذا المسهم بالفاعل، وقد يكون دور المسهم في إحداث الجريمة «ثانويًّا»، فتوصف مساهمته بأنها مساهمة تبعية، ويسمى هذا المسهم «الشريك» [٣]، وقد يكون دور المسهم لاحقًا على تمام الجريمة وإن ارتبط بها برباط وثيق ويسمى هذا المسهم بالمختبئ، ولكل مسهم من هؤلاء وضع قانوني معين وأحكام متميزة[٤].

بالإضافة إلى ذلك، يذهب الرأي الغالب فقهًا وقضاءً إلى أن المساعدة في كل صورها تطلب نشاطًا إيجابيًّا يبذله المساعد، ويقدم عن طريقة العون إلى الفاعل. أما الموقف السلبي المتمثل في التعود على الحيلولة دون وقوع الجريمة على الرغم من استطاعة ذلك، أو الامتناع عن إبلاغ أمرها إلى السلطات العامة قبل وقوعها كي تعمل على منعها، فهو غير كاف لتحقق المساعدة[٥]. وقد أكدت محكمة النقض المصرية ذلك في عبارة قاطعة مفادها أن الاشتراك في الجريمة لا يتكون إلا من أعمال إيجابية، ولا ينتج أبداً من أعمال سلبية[٦].

بناءً على ما تقدم؛ نجد أن الاستخدام غير المشروع لتقنية التزييف العميق واصطناع فيديوهات غير حقيقية للتشهير والانتقام من أحد الأشخاص والتي تمر بثلاث مراحل كما أسلفنا ذكره، وتتكون كل مرحلة من عدد من الجرائم ومن ثَمَّ فنحن بصدد تحديد

(١) د. محمود نجيب حسني: شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة، دار النهضة العربية، ١٩٦٢، ص ٤٣٢، د. محمد زكي أبو عامر، د. سليمان عبد المنعم: قانون العقوبات، القسم العام، دار الجامعة الجديدة، ٢٠٠٢، ص ٣٠١، أ. أحمد محمود عواد الوقاد: المساهمة الجنائية للقتل بالسم، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، ٢٠١٤، ص ٨.

(٢) د. محمود نجيب حسني: المساهمة الجنائية في التشريعات العربية، مطبعة جامعة القاهرة والكتاب الجامعي، ١٩٩٠، ص ٣٠١.

(٣) د. مدحت عبد العزيز: المسئولية الجنائية للاشتراك بالمساعدة، دراسة مقارنة، دار النهضة العربية، ٢٠١٢، ص ١٧.

(٤)د. محمد زكي أبو عامر: قانون العقوبات القسم العام، منشأة المعارف بالإسكندرية، ١٩٩٣، ص ٣٨٠.

(٥) د. محمود محمود مصطفي: شرح قانون العقوبات القسم العام، مطابع دار الكتاب العربي، القاهرة، ١٩٦٠، ص ٢٦٤.

(٦) نقض مصري ٢٨/ مايو/١٩٤٥، مجموعة القواعد القانونية، ج٦، رقم٥٨٣، ص٧١٩، الطعن رقم ٥٣٣٤ لسنه ٨٢ ق، الدوائر الجنائية، ٢٠١٣/١/١٣، مكتب فني (سنه ٦٤، قاعدة ١٢، ص٩٠).

مسئولية كل شخص في هذه المراحل والتي تبدأ بتجميع الصور والبيانات اللازمة لإنتاج الفيديـو، ثم استخدامها للتحريف والمعالجة، وأخـيرًا نشر هذه المقاطع بأية وسيلة من وسائل النشر وسنتناول ذلك في ثلاثة مباحث على النحو التالي:

- **المبحث الأول: المسئولية الجنائية لجامع البيانات الشخصية.**
- **المبحث الثاني: المسئولية الجنائية لمعالج ومنتج هذه الفيديوهات.**
- **المبحث الثالث: المسئولية الجنائية عن النشر.**

المبحث الأول

المسئولية الجنائية لجامع البيانات الشخصية

المسئولية الجنائية تعني عنصرين مهمين، أولهما مادي ويعني الإسناد المادي للفعل، وثانيهما شخصي، ويعني الإسناد المعنوي للفعل[١] وفقًا للإسناد المادي لا تنعقد المسئولية الجنائية إلا عن الفعل الشخصي، بينما إسناد المعنوي للفعل لا تنعقد معه المسئولية الجنائية إلا إذا اتجهت إرادة المسند إليه الفعل ماديًّا القيام بارتكاب الفعل[٢].

بادئ ذي بدء؛ فإن أول من يسأل جنائيًا هو جامع البيانات الشخصية[٣]، ويجب التفرقة بين جامع البيانات بحكم وظيفته، وجامع البيانات كشخص طبيعي لا يملك البيانات والصور إنما قائم على اصطيادها وجمعها.

الجدير بالذكر أن القانون المصري لحماية البيانات الشخصية رقم ١٥١ لسنه ٢٠٢٠ حظر كافة أعمال المعالجة والتحليل إلا بعد الحصول على موافقة الشخص المعني بهذه البيانات[٤]؛ حيث جاءت المادة الثانية من القانون تنص على: «لا يجوز جمع البيانات الشخصية، أو معالجتها، أو الإفصاح عنها، أو إفشائها بأية وسيلة من الوسائل إلا بموافقة صريحة من الشخص المعني بالبيانات، أو في الأحوال المصرح بها قانونًا»[٥].

أولاً- المسئولية الجنائية لجامع البيانات بحكم وظيفته:

لقد ميز القانون المصري لحماية البيانات الشخصية رقم ١٥١ لسنه ٢٠٢٠ بين المتحكم والحائز والمعالج، وذلك بتحديد مسئوليات والتزامات كل منهم، ولقد نص القانون عليهم في الفصل الأول، في التعريفات، في المادة الأولى: «الحائز: هو كل شخص طبيعي أو اعتباري، يحوز ويحتفظ قانونيًا أو فعليًا بيانات شخصية في أية صورة من الصور، أو على أية وسيلة تخزين سواءً أكان هو المنشئ للبيانات، أم انتقلت إليه حيازتها بأية صورة».

---

(١) د.ممدوح حسن العدوان: المسئولية الجنائية عن أفعال كيانات الذكاء الاصطناعي غير المشروعة، مجلة دراسات لعلوم الشريعة و القانون الجامعة الأردنية المجلد ٤٨، عدد ٤، ٢٠٢١، ص ١٥٥.

(٢) د.أحمد فتحي سرور: القانون الجنائي الدستوري، الطبعة الثانية، دار الشروق، ٢٠٠٢، ص ١٩٧.

(٣) د. محمود سلامه: مرجع سابق، ص ٤٣.

(٤) د.رزق سعد: الحماية الجنائية للبيانات الشخصية المعالجة إلكترونياً في ضوء القانون رقم ١٥١ لسنه ٢٠٢٠، ورقة بحثية مقدمة للمؤتمر العلمي الدولي «الحماية القانونية للإنسان في ضوء التقدم الطبي والتكنولوجي»، كلية الحقوق جامعة السادات، ٢٠٢٢، ص ٢٧.

(5) https://www.cc.gov.eg/legislation_single?id=404171

بينما المتحكم: هو 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 طبقًا للغرض المحدد أو نشاطه[١]، ولقد عرفته المادة الثانية في اللائحة العامة الأوروبية للبيانات (GPDR) بأنه : يعني الشخص الطبيعي أو الاعتباري أو السلطة العامة أو الوكالة أو أي شخص آخر، تحدد الهيئة بمفردها أو بالاشتراك مع آخرين أغراض ووسائل معالجة البيانات الشخصية ؛ عندما تحدد الأغراض ووسائل المعالجة التي يحددها قانون الاتحاد أو قانون الدول الأعضاء»[٢].

---

(١) أولاً: 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 قانونًا.

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

٣ – وضع طريقة وأسلوب ومعايير المعالجة طبقًا 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 قانونًا.

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 قِبَل 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 تبقى 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.

(2) ‹controller' means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes (…) and means of the processing of personal data; where the purposes (…) and means of processing are determined by Union law or Member State law, the controller or the specific criteria for his nomination may be designated by Union law or by Member State law.

كما عرف القانون المصري المعالج: بأنه: كل شخص طبيعي أو اعتباري مختص بطبيعة عمله، بمعالجة البيانات الشخصية لصالحه أو لصالح المتحكم بالاتفاق معه ووفقًا لتعليماته»[1]، وهو ذات التعريف في المادة الثانية في اللائحة العامة الأوروبية للبيانات (GPDR): «يعني شخصًا طبيعيًا، أو اعتباريًا، أو سلطة عامة، أو وكالة، أو أي شخص آخر أو الهيئة التي تعالج البيانات الشخصية نيابة عن المتحكم»[2].

ومن ثَمَّ نجد أن هؤلاء بحكم وظيفتهم يقومون بالتعامل مع البيانات إلا أن جمعها

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

١ – إجراء المعالجة وتنفيذها طبقًا 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 قانونًا.

٦ – عدم إجراء أية 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 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. راجع في ذلك نصوص القانون رقم ١٥١ لسنه ٢٠٢٠:
https://www.cc.gov.eg/legislation_single?id=404869

(2) ‹processor' means a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

واستخدامها لغير الغرض المخصص له هو من قبيل العمل غير المباح؛ حيث جاءت المادة الثالثة من ذات القانون سالف الذكر تنص على: «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»[١].

وبما أن الاستخدام هنا في التزييف العميق لغرض التشهير والانتقام من قبيل الأعمال غير المشروعة، من ثم يكونوا مسئولين مسئولية جنائية كاملة باعتبارهم فاعلين أصليين، وذلك لكونهم قد استخدموا واستحوذوا على بيانات شخصية بالمخالفة للقانون، بل إن قيامهم بجمع البيانات دون ترخيص[٢] أو تصريح[٣] يُعَدُّ فعلاً مجرمًا ويجعلهم ذوي مسئولية جنائية كاملة.

ليس ذلك فحسب، بل جاءت المادة السابعة من القانون سالف الذكر: «يلتزم كل من المتحكم والمعالج بحسب الأحوال حال علمه بوجود خرق أو انتهاك للبيانات الشخصية لديه بإبلاغ المركز خلال اثنتين وسبعين ساعة، وفي حال كان هذا الخرق أو الانتهاك متعلقًا باعتبارات حماية الأمن القومي فيكون الإبلاغ فوريًا، وعلى المركز وفي جميع الأحوال إخطار جهات الأمن القومي بالواقعة فورًا، كما يلتزم بموافاة المركز خلال اثنتين وسبعين ساعة من تاريخ علمه بما يأتي:

---

(1) https://www.cc.gov.eg/legislation_single?id=404171

(٢) الفصل الأول- التعريفات مادة (١)، الترخيص: هو كل 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 بأية صورة، وتحدد التزامات المرخص له وفق القواعد والشروط والإجراءات والمعايير الفنية المحددة باللائحة التنفيذية لهذا القانون، وذلك لمدة ثلاث سنوات قابلة للتجديد لمدد أخرى.

(٣) الفصل الأول- التعريفات مادة (١) التصريح: هو كل 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 بأية صورة، أو لأداء مهمة أو مهام معينة، وتحدد هذه الوثيقة التزامات المصرح له وفق القواعد والشروط والإجراءات والمعايير الفنية المحددة باللائحة التنفيذية، لمدة مؤقتة لا تجاوز سنة، ويجوز تجديدها لأكثر من مدة.

١- وصف طبيعة الخرق أو الانتهاك، وصورته وأسبابه والعدد التقريبي للبيانات الشخصية وسجلاتها.

٢- بيانات مسئول حماية البيانات الشخصية لديه.

٣- الآثار المحتملة لحادث الخرق أو الانتهاك.

٤- وصف الإجراءات المتخذة والمقترح تنفيذها لمواجهة هذا الخرق أو الانتهاك والتقليل من آثاره السلبية.

٥- توثيق أي خرق أو انتهاك للبيانات الشخصية، والإجراءات التصحيحية المتخذة لمواجهته.

٦- أية وثائق أو معلومات أو بيانات يطلبها المركز.

وفي جميع الأحوال يجب على المتحكم والمعالج، بحسب الأحوال، إخطار الشخص المعني بالبيانات خلال ثلاثة أيام عمل من تاريخ الإبلاغ وما تم اتخاذه من إجراءات»[١].

ثانيًا- المسئولية الجنائية للشخص العادي جامع البيانات:

بادئ ذي بدء فإن المعلومات والبيانات من الممكن أن يتم جمعها بدون سيطرة عليها بحكم الوظيفة أو غيرها وذلك بطريقتين وجب التمييز بينهما:

عن طريق جمع المعلومات بطريقة يدوية مع حفظ الصور والفيديوهات، إلا أننا نجد أنه لا يوجد أي نص مجرّم لجمع البيانات المتاحة على مواقع السوشيال ميديا بواسطة الأشخاص، وتعد من قبيل الأعمال التحضيرية، أي لا عقاب على تجميع البيانات[٢]، إلا أنه يعد شريكًا فى الجريمة التي تم استخدام تلك المعلومات فيها بواسطه التزييف العميق، ولقد جاءت المادة (٤٣) من قانون العقوبات المصري تقضي بأن من اشترك في جريمة فعليه عقوبتها ولو كانت غير التي تعمد ارتكابها متى كانت الجريمة التي وقعت بالفعل نتيجة محتملة للتحريض أو الاتفاق أو المساعدة التي حصلت؛ فإذا كان الاتفاق على جمع البيانات والفيديوهات الخاصة للضحية، فإن من المحتمل أن يرتكب الفاعل فبركة للفيديوهات أو ابتزاز أو انتقام من الضحية، ومن ثَمَّ يكون جامع البيانات شريكًا،

(1) https://www.cc.gov.eg/legislation_single?id=404171

(٢) د. محمود سلامة: مرجع سابق، ص ٤٦.

ومستخدم تقنية التزييف العميق هو الفاعل الأصلي، فالأصل أن مسئولية الشريك تتحدد بما قصد المشاركة فيه، غير أنه لما كانت جريمة الشريك تابعة لجريمة الفاعل الأصلي، لذلـك فإن الشريك لا يُعاقب إذا عـدل الفاعل عن إتمام الجريمة، ولو كان هذا العدول علـى غير إرادة الشريـك، كما أنه لا يُسأل إلا عن الجريمة التي وقعت فعلاً، ولو كان قد قصـد الاشتراك فـي جريمة أشد منها، ولقـد أكدت محكمة النقض هـذا الاتجاه في حكمهـا حيث قضت بأنه : «لما كان الاشـتراك بالاتفاق إنما يتكون من اتحاد نية الفاعل والشريك على ارتكاب الفعل المتفق عليه وهذه النية من مخبآت الصدور ودخائل النفس التـي لا تقـع عادة تحت الحس وليس لها أمارات ظاهرة، كمـا أن الاشتراك بالتحريض قد لا تكـون له سمات أو شواهد ظاهرة تدل عليه، ويتحقق الاشتراك بالمساعدة بتدخل الشريـك مع الفاعل تدخلاً مقصودًا يتجاوب صداه مع فعله، ويتحقق فيه معنى تسهيل ارتـكاب الجريمة الذى جعله الشارع مناطًا لعقاب الشريـك، وللقاضي الجنائي إذا لم يقـم على الاتفـاق أو التحريض أو المساعـدة دليل مباشر أن يستـدل على ذلك بطريق الاستنتاج والقرائن التي تقوم لديه ما دام هذا الاستنتاج سائغًا وله من ظروف الدعوى ما يبرره»[١].

عـن طريق استخدام برامج اختراق[٢] والدخول إلى نظام معلوماتي، ولعلَّ مصطلح الاختراق قد عرف وفقًا للقانون المصري رقم ١٧٥ لسنه ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات بأنه: «الدخول غير المرخص به، أو المخالف لأحكام الترخيص، أو الدخول بأيـة طريقـة غير مشروعة، إلى نظام معلوماتي أو حاسـب آلي أو شبكة معلوماتية، وما في حكمها»[٣].

كما نجد أنه من الممكن أن يتم اعتراض البيانات الشخصية.

وقـد عرف الاعتراضـ بأنه: «مشاهـدة البيانـات أو المعلومات أو الحصـول عليها،

---

(١) نقض جنائـي، الطعـن رقـم ٢٤٩٦٣ لسنه ٦٦ بتاريـخ ١٩٩٨/١٢/١٥، نقض جنائي، الطعـن رقم ٢٠٩٩٩ لسنـه ٦٦ بتاريخ ١٩٩٨/١٠/٨

(٢) تعـد أبـرز تلـك الوقائع ما تم في عـام ٢٠١٤، من قيام أحد الأشخاص باختراق منصة iCloud، وقـام بسرقة عدد من صور المشاهير ونشره ما يقارب ٥٠٠ صورة .

Franks (M.-A.): «‹Revenge Porn' Reform: A View from the Front Lines,» Florida Law Review, Vol. 69, 2017, p. 1253

(٣) الجريدة الرسمية – العدد ٣٢ مكرر (ج) في ١٤ أغسطس سنة ٢٠١٨

https://www.cc.gov.eg/legislation_single?id=386006

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»[١]. في هذه الحالة تكون مسئولية جامع البيانات مسئولية كاملة لمخالفته للنصوص القانونية وارتكابهم للجرائم المكونة لها وهي: جريمة الدخول غير المشروع[٢] لنظام معلوماتي[٣]، وجريمة الاعتراض غير المشروع[٤].

(١) الجريدة الرسمية – العدد ٣٢ مكرر (ج) في ١٤ أغسطس سنة ٢٠١٨
https://www.cc.gov.eg/legislation_single?id=386006

(٢) مادة (١٤): 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 المعلوماتي، تكون العقوبة الحبس مدة لا تقل عن سنتين، وغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين.

الجريدة الرسمية – العدد ٣٢ مكرر (ج) في ١٤ أغسطس سنة ٢٠١٨
https://www.cc.gov.eg/legislation_single?id=386006

(٣) النظام المعلوماتي: مجموعة برامج وأدوات معدة لغرض إدارة ومعالجة البيانات والمعلومات، أو تقديم خدمة معلوماتية.
الجريدة الرسمية – العدد ٣٢ مكرر (ج) في ١٤ أغسطس سنة ٢٠١٨.
المادة الأولى راجع نصوص ذلك القانون على: https://www.cc.gov.eg/legislation_single?id=386006

(٤) مادة (١٦): يُعاقب بالحبس مدة لا تقل عن سنة، وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتين وخمسين ألف جنيه، أو بإحدى هاتين العقوبتين، كل من اعترض بدون وجه حق أية معلومات أو بيانات أو كل ما هو متداول عن طريق شبكة معلوماتية أو أحد أجهزة الحاسب الآلي وما في حكمها.
الجريدة الرسمية – العدد ٣٢ مكرر (ج) في ١٤ أغسطس سنة ٢٠١٨.
https://www.cc.gov.eg/legislation_single?id=386006

المبحث الثاني

المسئولية الجنائية لمعالج ومنتج هذه الفيديوهات

بعـد انتهاء العمل مـن تصيد البيانات وجمـع المعلومات بشتى صورهـا، يبدأ العمل فـي المرحلـة الثانية فتتم معالجة البيانـات، ومن ثم صنع الفيديـو المفبرك عن طريق خوارزميـات الـذكاء الاصطناعي؛ حيـث يتم تطعيـم البرنامج بصـور للضحية، يكون موضح خلالها حركات الوجه والإيماءات الخاصة به حتى يضحى الفيديو كأنه حقيقي، ويُرفـق معها الفيديـو المراد تركيب الصـور عليه ليقول ما لا يقولـه، ويفعل ما لم يقوم بفعله.

ومن ثـم تكون مسئولية مغـذي البرنامج بالصـور والفيديوهـات لمعالجتها وتكوين فيديو مفبرك مسئولية جنائية كاملة، ويكون بذلك هو الفاعل الأصلي في الجريمة[١].

والجدير بالذكر أن المادة (٢٦) من ذات القانون سالف الذكر تؤكد على تجريم ذلك الفعـل؛ حيـث نصت على أنه:«يُعاقـب بالحبس مدة لا تقل عن سنتـين ولا تجاوز خمس سنـوات وبغرامـة لا تقل عن مائـة ألف جنيه ولا تجـاوز ثلاثمائة ألف جنيـه أو بإحدى هاتين العقوبتين 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[٢]».

بل وجاءت المادة (٣٦) من القانون رقم ١٧٥ لسنه ٢٠١٨ تجرِّم وتؤكد على المسئولية الجنائية الكاملة للشخص الاعتباري حيـال معالجة البيانات وتسهيل ارتكاب الجريمة وجعلتـه فاعلاً أصليًا في هذه الجريمة: «في الأحوال التي ترتكب فيها أي من الجرائم المنصوص عليها في هذا القانون، باسم ولحساب الشخص الاعتباري، يُعاقب المسؤول عن الإدارة الفعلية إذا ثبت علمه بالجريمة أو سهل ارتكابها تحقيقًا لمصلحة له أو لغيره بذات عقوبة الفاعل الأصلي».

---

(١) د. محمود سلامه: مرجع سابق، ص٤٨.

(٢) الجريدة الرسمية – العدد ٣٢ مكرر (ج) في ١٤ أغسطس سنة ٢٠١٨
https://www.cc.gov.eg/legislation_single?id=386006

ويتبادر إلى ذهننا تساؤل مهم: ما مدى مسئولية صانع ومبرمج البرنامج المستخدم في التزييف العميق كجريمة محتملة ناتجه عن إساءة استعمال البرنامج؟

للإجابة على ذلك التساؤل نستعرض حكم محكمة النقض المصرية على النحو التالي:

حيث وضعت محكمة النقض المصرية أساس المسئولية الجنائية عن الجرائم المحتملة في ضرورة وجود جريمة أصلية، فجاء حكمها كما يلي: «قيام الجريمة الاحتمالية قبل المتهم رهن بثبوت مساهمته في جريمة أصلية قصد إليها فاعلاً كان أم شريكًا»[١].

وجاء في حكم آخر أيضًا: «... جعل المتهم مسئولًا أيضًا عن النتائج المحتملة لجريمته الأصلية، متى كان في مقدوره، أو كان من واجبه أن يتوقع حدوثها على أساس افتراض أن إرادة الجاني لا بد أن تكون قد توجهت نحو الجرم الأصلي، ونتائجه الطبيعية...»[٢].

ويتضح من خلال الحكمين السابقين أن القضاء قد جعل أساس وجود الجرائم المحتملة هو وجود جرائم أصلية، وأساس ذلك أن الشارع المصري لا يأخذ بالقصد الاحتمالي إلا في الحالات التي يؤاخذ فيها على الجريمة التي تجاوز النتيجة فيها قصد الجاني ولو لم يتوقعها، أو في الحالات التي يتوقع فيها الشخص حصول النتيجة الإجرامية، ومع ذلك يقدم على فعله، وليكن ما يكون ويرتضي حصول تلك النتيجة إن حصلت وإن كان يتمنى عدم حصولها[٣].

وبناءً على ما تقدم ذكره؛ يكون مبرمج البرنامج غير مسئول جنائيًّا عن فعله مالم يشكل جريمة في بادئ الأمر.

(١) الطعن رقم ٦٠٠٧ لسنة ٥٨ ق جلسة ١٩٨٨/١٢/٨. مكتب فني سنة ٣٩ - قاعدة ١٩٥ - ص ١٢٦١.

(٢) الطعن رقم ١٥٣٢١ لسنة ٨٥ قضائية، الدوائر الجنائية - جلسة ٢٠١٦/٢/٣، مكتب فنى سنة ٦٧ - قاعدة ٢١ - ص ١٥٣ .

(٣) د.عبد العظيم مرسي وزير: شرح قانون العقوبات - القسم العام، الجزء الأول، الطبعة الثامنة، دار النهضة العربية، ٢٠١٠، ص ٤١٨.

المبحث الثالث

المسئولية الجنائية عن النشر

بعـد انتهاء المرحلة الثانية، وهي تلفيـق الفيديوهات وصنع فيديوهات مفبركة تأتي المرحلـة الثالثة وهي إظهار تلـك الفيديوهات إلى الواقع والعلـن، فـي بادئ الأمر يجب التفرقـة بين طرفين رئيسيين، هما: الناشر ومدير الموقع، وسنتناول مسئولية كل منهما على النحو الآتي:

أولاً- المسئولية الجنائية للناشر:

مما لا جدال فيه؛ أن مسئولية الناشر مسئولية جنائية كامله ولعلَّ نص المادة (٢٥) مـن القانـون المصري رقـم ١٧٥ لسنه ٢٠١٨ جاء قاطع الدلالة علـى ذلك؛ حيث نصت علي: «يُعاقب 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 القيـم الأسرية فـي المجتمع المصري، أو انتهك حرمة الحياة الخاصة أو أرسل بكثافة العديد مـن الرسائل الإلكترونية لشخص معين دون موافقتـه، أو منح بيانات شخصية إلى نظـام أو موقع إلكتروني لترويج السلع أو الخدمات دون موافقته، أو نشر عن طريق الشبكـة المعلوماتية أو بإحدى وسائـل تقنية المعلومات معلومات أو أخبـارًا أو صورًا وما فـي حكمها، تنتهـك خصوصية أي شخص دون رضاه، سواء كانـت المعلومات المنشورة صحيحة أم غير صحيحة»[(١)].

وبالإمعـان فـي نص تلك المادة نجد أن القانون قـد جرّم النشر دون النظر إلى عدد مـن تم إعلامهـم بتلك الفيديوهات والصور، مما يعنـي أن النشر جريمة حتى ولو كان من اطلع على تلك الصورة شخصًا واحدًا[(٢)].

الجديـر بالذكر أن محكمة الطفـل بطنطا فـي جلستهـا (٢٤ مارس ٢٠٢٢) عاقبت المتهم السادس بالحبس لمدة (٥) سنوات، وتضمن الحكم بالحبس لمدة سنتين عن تهمة

(١) الجريدة الرسمية – العدد ٣٢ مكرر (ج) في ١٤ أغسطس سنة ٢٠١٨
https://www.cc.gov.eg/legislation_single?id=386006

(٢) د. أحمد زكير: مرجع سابق، ص٢٢٧٣.

هتك العرض، وحبسه ثلاث سنوات عن استعمال صور خاصة ونشرها، والتعدي على المبادئ الأسرية[١].

ثانيًا- المسئولية الجنائية لمدير الموقع:

عرف القانون المصري رقم ١٧٥ لسنه ٢٠١٨ 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[٢]».

حتى يتسنى لنا معرفة مدى مسئولية مدير الموقع جنائيًّا نستعرض نص المادة (٢٧) من القانون رقم ١٧٥ لسنه ٢٠١٨: «يُعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن مائة ألف جنيه، ولا تزيد عن ثلاثمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من أنشأ أو أدار أو استخدم موقعًا أو حسابًا خاصًا على شبكة معلوماتية يهدف إلى ارتكاب أو تسهيل ارتكاب جريمة معاقب عليها قانونًا[٣]».

---

(١) حكم محكمة الطفل بطنطا القضية رقم ٤ لسنه ٢٠٢٢، جلسة ٢٤ مارس سنه ٢٠٢٢.

قرار الإحالة: كان المستشار المحامي العام لنيابة غرب طنطا، بمحافظة الغربية قد أحال المتهم السادس ويدعى «محمود.ع.س» طالب بالصف الأول الثانوي ويبلغ من العمر ١٦ عاما، في واقعة الطفلة بسنت خالد شلبي، بمحافظة الغربية، إلى محكمة الطفل بطنطا، وجاء في أمر الإحالة أن المتهم ارتكب جريمة هتك عرض المجني عليها بغير قوة ولاتهديد والتي لم تبلغ من العمر ١٨عامًا بأن استطال عموم جسدها وعموم عفتها.

فلقد قضت المحكمة في حكمها الصادر يوم الخميس الماضي، على المتهم السادس ويدعي (م.س)، «حدث» البالغ من العمر ١٦ عامًا، ومقيد بالصف الأول الثانوي، في قضية بسنت خالد شلبي، المعروفة إعلاميًا بضحية «الابتزاز الإلكتروني» بالغربية، بالسجن لمدة سنتين عن التهمة الأولى، هتك عرض، وبراءة من التهمة الثانية، الاعتداء على حرمة الحياة الخاصة، وثلاث سنوات عن التهم: الثالثة، والرابعة والخامسة، وهى نشر صور، وتعمد مضايقة المجني عليها، وتعديه على القيم والمبادئ الأسرية.

https://www.almawq3.com/%D8%A7%D9%84%D8%A5%D8%B3%D8%AA%D8%A6%D9%86%D8%A7%D9%81-%D8%AA%D8%A3%D9%8A%D9%8A%D8%AF-%D8%A7%D9%84%D8%AD%D9%83%D9%85-%D8%B9%D9%84%D9%8A-%D8%A7%D9%84%D9%85%D8%AA%D9%87%D9%85-%D8%A7%D9%84%D8%B3%D8%A7/?utm_source=rss&utm_medium=rss&utm_campaign=%25d8%25a7%25d9%2584%25d8%25a5%25d8%25b3%25d8%25aa%25d8%25a6%25d9%2586%25d8%25a7%25d9%2581-%25d8%25aa%25d8%25a3%25d9%258a%25d9%258a%25d8%25af-%25d8%25a7%25d9%2584%25d8%25ad%25d9%2583%25d9%2585-%25d8%25b9%25d9%2584%25d9%258a-%25d8%25a7%25d9%2584%25d9%2585%25d8%25aa%25d9%2587%25d9%2585-%25d8%25a7%25d9%2584%25d8%25b3%25d8%25a7

(٢)الجريدة الرسمية – العدد ٣٢ مكرر (ج) في ١٤ أغسطس سنة ٢٠١٨
https://www.cc.gov.eg/legislation_single?id=386006

(٣) الجريدة الرسمية – العدد ٣٢ مكرر (ج) في ١٤ أغسطس سنة ٢٠١٨
https://www.cc.gov.eg/legislation_single?id=386006

ليس ذلك فحسب بل نصت المادة (٢٩) على: «يُعاقب بالحبس مدة لا تقل عن سنة، وبغرامـة لا تقـل عن عشريـن ألف جنيه ولا تجـاوز مائتي ألف جنيـه، أو بإحدى هاتين العقوبتين كل مسئول عن إدارة الموقع أو الحساب الخاص أو البريد الإلكتروني أو النظام المعلوماتـي عَرَّض أيًا منهم لإحـدى الجرائم المنصوص عليها في هذا القانون، ويُعاقب بالحبـس مـدة لا تقل عن ستة أشهـر، وبغرامة لا تقل عن عشـرة آلاف جنيه ولا تجاوز مائـة ألف جنيـه، أو بإحدى هاتين العقوبتـين، كل مسئول عـن إدارة الموقع أو الحساب الخاصـ أو البريد الإلكتروني أو النظام المعلوماتي تسبب بإهماله في تَعرّض أي منهما لإحـدى الجرائم المنصوص عليها فـي هذا القانون، وكان ذلك بعـدم اتخاذه التدابير والاحتياطيات التأمينية الواردة في اللائحة التنفيذية لهذا القانون»[١].

بالإمعان فيما تقدم؛ نجد أن مدير الموقع مسؤول جنائيًّا عن المعلومات المنشورة على المواقع والحسابات الخاصة سواء كان بإرادته أو بإهمال منه.

لعـلَّ التسـاؤل المهـم: مـا المسئوليـة الجنائية حيـال نشرها علـى مواقـع التواصل الاجتماعي؟

فـي بدايـة الأمر؛ عـرف التواصل الاجتماعي بأنـه «هو تبادل المحتـوى الذي يحمل الطابـع الشخصـي، حيـث يكون بين طرفـين أو أكثر يسمـى أحدهمـا بالمرسل والآخر بالمستقبـل»[٢]، لـذا عرفت مواقـع التواصـل الاجتماعي بأنهـا (شبـكات اجتماعية[٣] تفاعلية، تتيح التواصل لمستخدميها في أي وقت، وفي أي مكان في العالم، ظهرت على شبكـة الإنترنت منذ سنـوات، وتمكنهم مـن التواصل المرئي والصوتـي وتبادل الصور

(١) الجريدة الرسمية – العدد ٣٢ مكرر (ج) في ١٤ أغسطس سنة ٢٠١٨
https://www.cc.gov.eg/legislation_single?id=386006

(٢) د.أيمـن أحمد الدلوع: المسؤولية المدنية الناشئة عن الممارسات غير المشروعة عبر مواقع التواصل الاجتماعي، كلية الدراسات الإسلامية والعربية للبنات بالإسكندرية، المجلد السابع، ع ٣٢، ص ٩٣٧.

(٣) لعـل مفهـوم الشبكات الاجتماعية ووسائل التواصل الاجتماعي مختلفة وشاسعة، حيـث إن مصطلح الشبكات الاجتماعية هي الأعـم والأشمـل فالشبكات تحتوي على وسائل التواصل، بمعنى أوضح من ذلـك أنها صور من صور الشبكات؛ حيث إن وسائل التواصل الاجتماعي يمكن استخدامها عن طريق الموقع الإلكتروني أو التطبيقات الموجودة على المتاجر الإلكترونية.
د.حسن مصطفى حسن: مدخل إلى الإعلام الجديد تطابقات وتطبيقات، ط١، مكتبة الآفاق المشرقة، الإمارات، ٢٠١٦، ص ١٨.
د.سيف مجيد العاني: مسؤولية المستخدم الجزائية عن جرائم وسائل التواصل الاجتماعي، دراسة مقارنة، دار دروب المعرفة، ٢٠٢٢، ص ٢٣.

وغيرها من الإمكانات التي توطد العلاقات الاجتماعية بينهم)[١]، تشير تلك المواقع إلى النشر الواسع للمحتوى، على الرغم من أن المعلومات المضللة والمعلومات الخاطئة كانت دائمًا مشكلة، حيث إن المعلومات يمكن أن تنتقل عبر شبكات التواصل الواسعة بشكل أسرع من أي وقت مضى[٢]؛ حيث بلغ عدد المستخدمين لتلك المواقع في عام ٢٠٠٤ أكثر من مليون مستخدم أمريكي، وعندما بدأت في الانتشار في كافة البلاد أصبح العدد في ٢٠١٠ (٥٠٠) مليون مستخدم[٣]، كما بلغ عدد مستخدمي الفيس بوك من الشباب العربي نحو ٢٧ مليون شاب[٤]، لقد وصل عدد حسابات أحد المواقع (Facebook) في سنة ٢٠١٤ إلى ١,٣٥ مليار حساب[٥]، وفي عام ٢٠١٨ نجد أن الإحصاءات تشير إلى أن (٥) مليارات شخص حول العالم قاموا بالاتصال وإرسال واستقبال الرسائل النصية والتغريد والتصفح على الهواتف المحمولة، وأن عدد مستخدمي السوشيال ميديا بلغ ثلاثة مليارات نسمة[٦]. فقد أظهرت الدراسات أن المعلومات الخاطئة تصل إلى عدد أكبر من الناس وتنتشر بشكل أسرع من الحقيقة[٧].

ومن ثم في ضوء انتشار تلك المواقع والدور المهم التي تقوم به، فكان لا بد من التطرق إلى مسئولية نشر المحتوى المزيف على شبكات التواصل الاجتماعي سواء أكان ذلك النشر على حسابات الشخص ذاته أم عن طريق صفحات أو مجموعات آخرى، إلا أنه بطبيعة الحال يعد الشخص مسئولاً عمَّا قام بنشرة في أي منهما[٨].

تطبيقًا على ذلك: قررت محكمة جنايات الجيزة، بمعاقبة الشاب المتهم بتهديد

---

(١) أ.طه حازم الصفدي: المسؤولية الجزائية عن إساءة استخدام وسائل التواصل الاجتماعي (دراسة تحليلية مقارنة في ضوء الأنظمة القانونية المعاصرة والشريعة الإسلامية)، رسالة ماجستير، كلية الشريعة الإسلامية، الجامعة الإسلامية بغزة، ٢٠١٩، ص ٢٠.

د. عبد الرازق محمد الدليمي: الإعلام الجديد والصحافة الإلكترونية، دار وائل للنشر، ط١، ٢٠١١، ص ١٨٣.

(2) Vosoughi, Soroush, Deb Roy, and Sinan Aral: «The spread of true and false news online.» science 359.6380 -2018: p 1146

(3) [0]Sabrina Laroche: Les médias sociaux, nouveau canal d'influence dans la stratégie relationnelle desmarques , Université de Strasbourg , Institut d'Etudes Politiques de Strasbourg , Mémoire ,JUIN 2012 ,p.6.

(٤) د.مجدي محمد الداغر: مرجع سابق، ص ٥٢٩.

(5) Valère Ndior: Le réseau social: essai d'identification et de qualification_Droit et réseaux sociaux_p18

(6) Simon Kemp: DIGITAL IN 2018: WORLD'S INTERNET USERS PASS THE 4 BILLION MARK -30 Jan 2018-https://wearesocial.com/uk/blog/2018/01/global-digital-report-2018/

(7) David Greene: We Don't Need New Laws for Faked Videos, We Already Have Them, ELECTRONIC FRONTIER FOUND. https://www.eff.org/deeplinks/

(٨) أ. صالح عبد الكريم: المسئولية الجنائية للناشر الإلكتروني على مواقع التواصل الاجتماعي، مجلة القرطاس، ع١٧ لسنة ٢٠٢٢، ص٢٦.

وابتـزاز فتـاة في بولاق الدكـرور بالسجن ثلاث سنوات عما أسند إليـه من نشره صورًا خادشه للحياء خاصة بالفتاة على مواقع التواصل الاجتماعي «فيسبوك» و«واتس آب» [١]

وفـي ذات السيـاق عاقبت هيئة محكمـة جنايات سوهاج فـي جلستها ٢٠٢٣/٥/٦ العاطـل «ع.أ.م» بالسجـن (٥) سنوات لاتهامـه بتهديد المجنى عليهمـا الفتاتين «ج خ» و«ر.ش»، والاعتداء على حرمة الحياة الخاصة بهما وإفشاء أمور مخدشة للشرف، بنشر صور خاصة لهما على موقع التواصل الاجتماعي فيس بوك بدائرة مركز المنشأة[٢].

إلا أن إشكالية مشاركة المحتوى وتداوله بين عدد من الأفراد يدعونا إلى تساؤل كيف تتحقـق تلك المسئولية قبلهم، فـي ظل عدم وجود أي نص يجـرِّم مشاركة المحتوى وإن ذلـك لا يعد اتفاقًا على ارتكاب جريمة بل هو مجرد توافق، ولقد فرقت محكمة النقض بينهـم فـي العديد من الأحكام؛ حيـث قضت بأنه: «وكان من المقـرر أن الاتفاق يتطلب تقابـل الإرادات تقابـلاً صريحًا علـى أركان الواقعة الجنائية التـي تكون محلاً له، وهو غـير التوافـق الذى لا يعدو مجرد توارد خواطر الجناة على ارتكاب فعل معين ينتويه كل واحـد منهم في نفسه مستقلاً عن الآخريـن، دون أن يكون بينهم اتفاق سابق، ولو كان كل منهـم على حدة قد أصر على ما تواردت الخواطر عليه، وهو ما لا يستوجب مساءلة سائر من توافقوا على فعل ارتكبه بعضهم إلا في الأحوال المبينة في القانون على سبيل الحصـر»[٣] فمن ثم إذا كان هنـاك إتفاق بينهم على نشر ذلك الفيديو المزيف يكونون مساهمين ويُعاقبون على نشر مثل هذه المقاطع، بينما إذا كان ذلك مجرد توارد خواطر فيعدُّ توافقًا ولا عقاب لهم.

وفي تطور سريـع لمنع تلك الجرائم قامت بعض شركات التواصل الاجتماعي بتغيير شروطهـا وأحكامها في محاولة للحد من انتشـار التزييف العميق؛ حيث أعلن Twitter مؤخـرا عن سياستـه الجديدة بشـأن «الوسائط الاصطناعية والتلاعـب بها»[٤]، ليس

(١) حكم محكمة جنايات الجيزة في القضية رقم ١١٣٧ لسنه ٢٠٢٢، جلسة ٢٠٢٢/٩/٢٦

(٢) تعود أحداث الواقعة لشهر يوليو من العام الماضي، عندما وجهت الجهات المختصة بمحافظة سوهاج للمتهم «ح. ص» سن ٢٦ عامًـا، عامـل تهمة تهديد المجني عليها «أ.ع» كتابـة عبر وسائل التواصل الاجتماعي باستخـدام تطبيقي ماسنجر وواتس آب، بإفشاء أمور خادشة للحياء وماسة للشرف، ونشر صور ومقاطع مرئية فاضحة لابنته «أ.أ»، وكان ذلك مصحوبًا بطلب الموافقة على عودته لخطبة نجلته رغمًا عنها، عقب إنهاء الخطبة من قبل العائلة.

(٣) نقض جنائي، الطعن رقم ١٦٤٧١ لسنه ٨٧ بتاريخ ٢٠١٨/١٠/٩، الطعن رقم ١٠٤٤ لسنه ٨١ بتاريخ ٢٠١٢/٣/١٥.

(4) Sinduja Rangarajan: WhatsApp Is a Petri Dish of Coronavirus Misinformation, MOTHER JONESHttps://www.motherjones.com/media/2020/03/whats app-

Felix T. Wu: Collateral Censorship and the Limits of Intermediary Immunity, 87 NOTRE DAME L. REV. 293,2013,p 300.

ذلك فحسب؛ حيث تنطبق سياسةTwitter[١] على «التزييف الرخيص» أيضًا[٢].

كما أعلن «تويتر» أنه سينظر فيما إذا كان المحتوى «تتم مشاركته بطريقة خادعة» وما إذا كان المحتوى «من المحتمل أن يؤثر على سلامة الجمهور، أو يتسبب في ضرر جسيم». ولقد طبق تويتر سياسته لأول مرة فعليًّا على مقطع فيديو للمرشح جو بايدن، حيث قام بنشره أحد أعضاء فريق حملة الرئيس ترامب، فلقد قام بقص الفيديو لقطع نهاية جملة بايدن، فبدا وكأنه يؤيد ترامب. ولقد أضاف تويتر علامة «وسائط تم التلاعب بها» إليها – بعد ١٨ ساعة من نشر التغريدة، وعند هذه النقطة شاهدها ٥ ملايين شخص[٣]، ولعلَّ كل هذه الاحتياطات كلها تعمل على منع نشر التزييف العميق، وإن كانت لم تكن كافية.

(١) بدأ ذلك الموقع في يوليو ٢٠٠٦ عن طريق جاك دروسي (Jack Dorsey) وعدد من قرنائه في العمل في شركة أوديو الأمريكية، ويتم تبادل الرسائل النصية من خلاله، وتُسمى tweets أي تغريدات، وتتكون الرسائل من ١٤٠ حرفًا فقط وتكون متاحة لجميع المشاركين، ولقد ارتفعت تلك الرسائل إلى أربع مليارات رسالة في عام ٢٠١٠، بمعنى أن المعلومات يتم نشرها على ذلك الموقع بواسطة المستخدمين، ويكون أغلبهم مستقبلين لها.

(2) Anna Yamaoka-Enkerlin: DISRUPTING DISINFORMATION: DEEPFAKES AND THE LAW LEGISLATION AND PUBLIC POLICY Vol. 22:725 ,p744.

(3) Taylor Hatmaker: Facebook Flags Biden Video from Trump's Social Media Di- rector as 'Partly False,' TECH-CRUNCH https://tech crunch.com/2020/03/09/facebook-biden-video-twitter-trump/.

الخاتمة

- أدت الظواهر الإجرامية المستحدثة باستخدام التقنيات الحديثة إلى بروز أنماط غـير مألوفة من الجرائم، والتـي لم يفرض لها قانون العقوبات القواعد العقابية اللازمة، كما أضاف اقتران تلك التقنيات بثورة الاتصالات التي تتصف بخاصية معقـدة وهـي عدم خضوعهـا للحـدود السياسية بعـدًا آخر من التعقيـد، الأمر الـذي قد يؤدي إلى عجز قانون العقوبـات عن توفير الحماية الجنائية للمصالح المشروعـة. الأمر الذي يعنى تحليل وتقييـم التشريع الجنائي وبيان مدى فاعليته في حماية المصالح الاجتماعية بهدف تطويره ومعالجة أوجه القصور فيه.
- إن جرائـم الذكاء الاصطناعى بوصفها جرائـم مستحدثة تتطور بسرعة؛ لذلك يجـب أن يواكب القانـون الجنائي هذا التطور في هذه الجرائم، ويعالج القصور فـي نصوصـه لمواجهتهـا؛ حفاظًا على الحقـوق المشروعة التـي يصيبها الضرر الكبـير من جراء تلك الجرائم، وإن تقنية التزييـف العميق تعد إحدى تطبيقات الـذكاء الاصطناعي؛ لذا كانت دراستنـا في هذا البحث عن إساءة استخدامها، ولقد خلصت إلى عدة نتائج مهمة وتوصيات نستعرض أهمها:

أولاً- أهم النتائج:

- إن الثـورات التكنولوجيـة تميل إلى خلق مواقف غالبًا ما تـؤدي إلى ضعف القيم الأخلاقيـة؛ حيث تمر الأسس والقيم الثقافية والسياسية والاجتماعية في جميع أنحـاء العالم بتغيير صامت، ولكنه هائل مع ظهـور منتجات الحاسوب الجديدة في السوق والثورة تكتسب زخمًا.
- إن أنشطة تقنية التزييف العميق متعاقبة؛ حيث إن الفيديوهات المزيفة لا تتم إلا بعـد عملية رصد وتتبع للصور والفيديوهات المنشورة قبل المجني عليه، ثم العمل على تحريف تلـك الفيديوهات والتلاعب بها واستخدامهـا في ابتزاز ومساومة المجني عليهم ثم نشرها.
- أن كلمـة التزييف العميق تنقسم إلى شقين «DEEP» وهي تعني العميق نسبة إلى خوارزميات الـذكاء الاصطناعي ومستمدة من التعلم العميق «DEEP Learning والتعلـم الآلي «Machine Learning» والشق الثاني وهي كلمة « fake » أي المزيفة نسبه إلى تزييف تلك الفيديوهات.

- تعمل تقنية التزييف العميق عن طريق آلية محددة وفقًا لخوارزميتين: الأولى (generator) وتعمل على نسخ مقطع فيديو متطابق عن طريق استيراد وجه خارجي، ورصد صور مختلفة لحركة الشخص وتعابير الوجه، وتعمل الثانية(discriminator) على مراجعه جودة الفيديو.
- قد خلت التشريعات الأوروبية والعربية من أي نصوص تجريميه حول تقنية التزييف العميق إلاَّ في ولايات أمريكية، هم من أدرجوا تجريمًا لتلك التقنية، وهم ولاية فرجينيا كاليفورنيا نيويورك جورجينيا.
- يؤكد الأزهر الشريف أنه من المحرَّم شرعًا والمجرَّم قانونًا استخدام البرامج والتقنيات الحديثة؛ سيّما تقنية «التزييف العميق Deep Fake»، في فبركة مقاطع مَرْئية أو مسموعة أو صور لأشخاص، بغرض ابتزازهم ماديًّا أو الطعن بها في أعراضهم وشرفهم، أو دفعهم لارتكاب أفعال محرَّمة.
- إن جرائم الاستخدام غير المشروع لتقنية التزييف العميق من الجرائم ذات الطابع الدولي؛ حيث الاعتماد على برامج مختلفة من خلال شبكة الإنترنت التي تتسم بالعالمية والتي تؤدي إلى انتشار الفيديوهات على شكل واسع الانتشار في دول مختلفة.
- إن مسئولية الناشر مسئولية جنائية كاملة، ولعلَّ نص المادة (٢٥) من القانون المصري رقم ١٧٥ لسنه ٢٠١٨ جاء قاطع الدلالة على ذلك.
- مدير الموقع الإلكتروني مسؤول جنائيًا عن المعلومات المنشورة على المواقع والحسابات الخاصة به سواء كان بإرادته أو بإهمال منه.
- مسئولية مغذي البرنامج بالصور والفيديوهات لمعالجتها، وتكوين فيديو مفبرك مسئولية جنائية كاملة، ويكون بذلك هو الفاعل الأصلي في الجريمة.
- إن القانون المصري قد جرَّم نشر البيانات بدون رضاء صاحبها دون النظر إلى عدد من تم إعلامهم بتلك الفيديوهات والصور، مما يعني أن النشر وتجريمه ينعقد حتى ولو كان من اطلع على تلك الصورة شخصًا واحدًا.
- تُعد جريمة معالجة البيانات من جرائم السلوك والتي لا تتطلب تحقيق نتيجة

وإنما يكتفي بأن يصدر عن الجاني السلوك الإجرامي، والذي يتمثل فى استعمال وسيلة تقنيه والتي تتمثل هنا فى تقنية التزييف العميق ومعالجة البيانات وربطها بمحتوى منافٍ للآداب، أو المساس بالشرف.

- يُقصد بالتضليـل الإعلامي كل كذب أو تشويه وإخفاء الحقائق عن الرأي العام، ويكـون ذلـك بواسطـة عرض المنتـوج عن تقنيـة التزييـف العميق عـبر المواقع الإلكترونية أو وسائل التواصل الاجتماعي.

ثانيًا- أهم التوصيات:

- نناشـد المشرع المصـري بتعديل نص المادة الأولى من القانـون ١٧٥ لسنه ٢٠١٨ والمعرفة لتقنية المعلومات لتشمل تقنية التزييف العميق والنص عليها صراحة.
- عمل حملات توعوية عن أخطار استخدام تلك التقنية، وعقد ندوات تعريفية بها منعًا لوقوع أي شخص في براثنها.
- ضـرورة عقد اتفاقيات دولية لوضع أسس فـي التعامل مع القائمين على ارتكاب الجرم عبر الحدود.
- العمـل علـى سن نصوص تجريمية صريحة تواجهـه الاستخـدام السيئ لتقنية التزييف العميق.
- ضـرورة العمـل علـى إيجاد وسائـل تُسانـد الطب الشرعـي في تحليـل وتفنيد الفيديوهات المفبركة.
- العمـل على استخدام التقدم التكنولوجي الهائل، واستخدام الذكاء الاصطناعي لمواجهـه مساوئ تلك التقنية حتى تكون المواجهـة من ذات فصيل الجريمة، وهو استخدام الذكاء الاصطناعي.

قائمة المراجع

أولاً- أهم المراجع القانونية العربية:

أ) الكتب العلمية:

- **د. أحمد عبد الظاهر:** الحماية الجنائية لحق الشخص المعنوي في الشرف والاعتبار، دار النهضة العربية، ٢٠٠٥.
- **د. أحمد فتحي سرور:** الوسيط في قانون العقوبات، القسم العام، الطبعة السادسة، نادي القضاة، ٢٠١٥.
- **د. أحمد فتحي سرور:** القانون الجنائي الدستوري، الطبعة الثانية، دار الشروق، ٢٠٠٢.
- **د. تامر صالح:** الابتزاز الإلكتروني، دراسة تحليليه مقارنة، دار الفكر والقانون، ٢٠٢١.
- **د. جميل عبد الباقي الصغير:** القانون الجنائي والتكنولوجيا الحديثة، دار النهضة العربية، ١٩٩٢.
- **د. حاتم عبد الرحمن:** الإجرام المعلوماتي، دار النهضة العربية، القاهرة، ٢٠٠٢.
- **د. حسام الدين محمد أحمد:** الحماية الجنائية للمبادئ الحاكمة للانتخابات السياسية في مراحلها المختلفة، دار النهضة العربية، ٢٠٠٢.
- **د. حسن مصطفى حسن:** مدخل إلى الإعلام الجديد تطابقات وتطبيقات، ط١، مكتبة الآفاق المشرقة، الإمارات، ٢٠١٦.
- **د. خالد حسن أحمد لطفي:** الدليل الرقمي ودوره في إثبات الجريمة المعلوماتية/ دار الفكر الجامعي، ٢٠١٩.
- **د. رأفت جوهري رمضان:** المسئولية الجنائية عن أعمال وسائل الإعلام، دار النهضة العربية، ٢٠١١.

- **د. زكـي زكي زيدان:** حـق المجني عليه فـي التعويض عن ضـرر النفس فـي الفقه الإسلامي والقانون الوضعي، دار الكتاب القانوني، ٢٠٠٩.
- .....: المدخل لدراسة الفقة الإسلامي، التركي للطباعة، ٢٠٠٠.
- **د. سامح السيد جاد:** شرح قانون العقوبات، القسم العام، دون دار نشر، ٢٠٠٥.
- **د. سليمـان عبـد المنعم:** أصـول علم الإجـرام القانـوني، دار الجامعة الجديدة للنشر، الإسكندرية، ١٩٩٤.
- **د. سليمـان محمـد الطماوي:** الجريمـة التأديبيـة – دراسة مقارنـة، دار الفكر العربي، ١٩٧٥، مصر.
- **د. سيـف مجيد العاني:** مسؤولية المستخدم الجزائية عن جرائم وسائل التواصل الاجتماعي، دراسة مقارنه، دار دروب المعرفة، ٢٠٢٢.
- **د. شريـف اللبـان:** تكنولوجيـا النشـر الصحفـي، الاتجاهات الحديثـة، الدار المصرية اللبنانية، ٢٠٠١.
- **د. شريـف سيـد كامل:** الجرائم الصحافيـة فـي القانون المصـري، دار النهضة العربية، ١٩٩٤.
- **الشيخ محمد بن أحمد بن محمد:** الوجيز فـي إيضاح قواعد الفقه الكلية، مؤسسة الرسالة العالمية، بيروت، ط٤، ١٩٩٦.
- **د. شيريـن كـدواني، وشريهـان توفيق:** الإعـلام الرقمي تشريعـات وأخلاقيات النشر، العربية للنشر والتوزيع، بدون تاريخ نشر.
- **شيلا براون،** ترجمة أ. هدي فؤاد: الجريمة والقانون فـي ثقافة الإعلام، مجموعة النيل العربية، ٢٠٠٦.
- **د. شيمـاء عبـد الغني:** الحمايـة الجنائية للتعامـلات الإلكترونيـة، دار النهضة العربية، ٢٠٠٥.
- **د. طارق سرور:** جرائم النشر والإعلام، دار النهضة العربية، ٢٠٠٤.

- **د. عبد الرازق محمد الدليمي:** الإعلام الجديد والصحافة الإلكترونية، دار وائل للنشر، ط١، ٢٠١١.
- **د. عبد العزيز لطفي جاد الله:** الجريمة السيبرانية وحماية أمن المعلومات، مؤسسة المروة للنشر والتوزيع، ٢٠٢٢.
- **د. عبد العظيم مرسي وزير:** شرح قانون العقوبات – القسم العام، الجزء الأول، الطبعة الثامنة، دار النهضة العربية، ٢٠١٠.
- **د. عبد الفتاح بيومي حجازي:** الأحداث والإنترنت، دار الفكر الجامعي، الإسكندرية، ٢٠٠٠.
- .....: الجريمة في عصر العولمة، دار الفكر الجامعي، الاسكندرية، ٢٠٠٧.
- .....: الدليل الجنائي والتزوير في جرائم الكمبيوتر والإنترنت، دار الكتب القانونية، ٢٠٠٢.
- **د. عبد الله السعود السراني:** مهارات التحقيق في جرائم تزييف العملة، جامعة نايف العربية للعلوم الأمنية، ٢٠١٠.
- **د. على عبد القادر القهوجي، د. فتوح عبد الله الشاذلي:** شرح قانون العقوبات القسم العام، الكتاب الثاني المسئولية والجزاء، بدون دار نشر، ٢٠٠٤.
- **د. عمر الفاروق:** المشكلات الهامة في الجرائم المتصلة بالحاسب الآلي وأبعادها الدولية بدون دار نشر، ١٩٩٥.
- **د. عوض محمد:** قانون العقوبات، القسم العام، دار المطبوعات الجامعية، الإسكندرية، ١٩٩٨.
- **د. غنام محمد غنام:** القانون الجنائي وجرائم تقنية المعلومات، مطبعة جامعة المنصورة، ٢٠٠٨.
- **د. فتوح عبد الله الشاذلي:** المسئولية الجنائية، دار المطبوعات الجامعية، الإسكندرية، ٢٠٠٦.

- .....: قانون العقوبات، القسم العام، دار المطبوعات الجامعية، ١٩٩٨.
- **كلاوس شواب:** الثـورة الصناعيـة الرابعة-ملخصات لكتب عالميـة تصدر عن مؤسسة محمد بن زايد، ٢٠١٧.
- **مـاري شروتر:** الذكاء الاصطناعـي ومكافحة التطرف العنيـف: كتاب تمهيدي، المركز الدولي لدراسة الراديكالية، بدون تاريخ نشر.
- **المبـارك بن محمد بن الأثير:** النهاية في غريـب الحديث والأثر، ج٢، دار الكتب العملية، بيروت، ١٩٧١.
- **د. محمد الشوابكة:** جرائم الحاسوب والإنترنت، الجريمة المعلوماتية دار الثقافة للنشر والتوزيع، ٢٠١١.
- **محمد بن منظور:** لسان العرب، ج٩، بيروت، ١٩٩٨.
- **د. محمـد زكـي أبـو عامـر:** قانـون العقوبـات القسـم العـام، منشـأة المعارف بالإسكندرية، ١٩٩٣.
- **د. محمـد زكي أبو عامر، د. سليمـان عبد المنعم:** قانون العقوبات، القسم العام، دار الجامعة الجديدة، ٢٠٠٢.
- **د. محمـد هشـام أبو الفتوح:** الشائعـات في قانون العقوبـات المصري والقوانين أخرى، دار النهضة العربية، ١٩٩٥.
- **د. محمـود أحمـد طـه:** المواجهـة التشريعيـة لجرائـم الكمبيوتـر والإنترنـت دراسة مقارنة، دار الفكر والقانون، ٢٠١٢.
- **د. محمـود رجب فتـح الله:** شـرح قانـون مكافحة الشائعـات، دراسـة مقارنة، دار الجامعة الجديدة، الإسكندرية، ٢٠٢٠.
- **د. محمـود محمـد سويـف:** جرائم الـذكاء الاصطناعـي (المجرمـون الجدد)، دار الجامعة الجديدة، ٢٠٢١.

- **د. محمود محمود مصطفى:** شرح قانون العقوبات القسم العام، مطابع دار الكتاب العربي، القاهرة، ١٩٦٠.
- **د. محمود نجيب حسني:** المساهمة الجنائية في التشريعات العربية، مطبعة جامعة القاهرة والكتاب الجامعي، ١٩٩٠.
- .....: النظرية العامة للقصد الجنائي دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية، دار النهضة العربية، ٢٠٠٦.
- .....: شرح قانون العقوبات القسم العام، النظرية العامة للجريمة، دار النهضة العربية، ١٩٦٢.
- **د. مدحت رمضان:** الحماية الجنائية لشرف واعتبار الشخصيات العامة، دار النهضة، بدون تاريخ نشر.
- **د. مدحت عبد العزيز:** المسئولية الجنائية للاشتراك بالمساعدة، دراسة مقارنة، دار النهضة العربية، ٢٠١٢.
- **د. ممدوح عبد المطلب:** خوارزميات الذكاء الاصطناعي وإنفاذ القانون، دار النهضة العربية، ٢٠٢٠.
- **د. منصور عمر المعايضة:** المسؤولية المدنية والجنائية في الأخطاء الطبية، مركز الدراسات والبحوث، الرياض، ٢٠٠٤.
- **د. نائلة عادل قورة:** جرائم الحاسب الآلي الاقتصادية، دراسة نظرية وتطبيقية، منشورات الحاتي الحقوقية، ٢٠٠٥.
- **د. هدى حامد قشقوش:** القتل بدافع الشفقة، دراسة مقارنة، دار النهضة العربية، ٢٠٠٦.
- **د. هلالي عبد اللاه:** اتفاقية بودابست لمكافحة جرائم المعلوماتية، دار النهضة العربية، ٢٠٠٧.
- .....: شرح قانون العقوبات، القسم العام، دار النهضة العربية، ١٩٨٧.

- **الوزير أبي المظهر يحي الشيباني:** اختلاف الأئمة العلماء، ج٢، دار الكتب العلمية، بدون سنه نشر.

ب) المقالات والدوريات العلمية:

- **د. أحمـد سعد على البرعي:** تطبيقات الـذكاء الاصطناعي والروبوت من منظور الفقه الإسلامي، مجلة دار الإفتاء المصرية، مجلد١٤، ع٤٨، يناير ٢٠٢٢.
- **د. أحمـد عبد الـلاه المراغـي:** السياسة الجنائيـة لمواجهة الإشاعـات والأخبار الكاذبة، مجلة الدراسات القانونية، ع٥٤ ج٢.
- **د. أحمـد لطفـي السيد مرعـي:** انعكاسـات تقنيـات الـذكاء الاصطناعي على نظريـة المسئوليـة الجنائية (دراسـة تأصيلية مقارنة) مجلة البحـوث القانونية والاقتصادية، جامعة المنصورة، العدد٨٠، يونيو ٢٠٢٢.
- **د. أحمـد محمد الخولي:** المسئولية المدنية الناتجة عـن الاستخدام غير المشروع لتطبيقات الذكاء الاصطناعي، مجلة البحوث الفقهية والقانونية، أكتوبر٢٠٢١.
- **د. أحمـد مصطفى محـرم:** استخدامات الـذكاء الاصطناعـي استخدام تقنية التزييـف العميق في قذف الغـير، مجلة البحوث الفقهيـة والاقتصادية، أكتوبر ٢٠٢٢.
- **د. أرسـلاح ظفـري:** جريمـة الاعتداء على حـق الخصوصية عـبر الإنترنت في الشريعـة الإسلاميـة والنظام القانـوني الأفغاني: دراسة مقارنـة، مجلة ريحان للنشر العلمي، ع٢٦، ٢٠٢٢.
- **د. أسامـه بن غانم:** جريمـة الدخول غير المشروع إلى النظـام المعلوماتي، مجلة دراسات المعلومات، ع١٤، ٢٠١٢.
- **د. أسامـة عطيـة محمد عبـد العـال:** المسئوليـة الجنائية عن جريمـة التضليل الإعلامي، مجلة العلوم الاقتصادية والقانونية، ع١، السنه٦٣، يناير ٢٠٢١.
- **د. آلان بونيـه:** الذكاء الاصطناعي واقعه ومستقبلـه، كتب عالم المعرفة، المجلس الوطني للثقافة والفنون والآداب، الكويت، ع١٧٢، ١٩٩٣.

- **د. أيمن أحمد الدلوع:** المسؤولية المدنية الناشئة عن الممارسات غير المشروعة عبر مواقع التواصل الاجتماعي، كلية الدراسات الإسلامية والعربية للبنات بالإسكندرية، المجلد السابع، ع ٣٢.
- **د. جبريل العريشي:** استخدام البيانات الضخمة والذكاء الاصطناعي في مواجهة جائحة فيروس كورونا المستجد، المجلة العربية للدراسات الأمنية، العدد ٣٦ع، ٢٠٢٠ .
- **د. جيهان صبري محمد عبد الغفار:** الحكم الشرعي للمخدرات الرقمية، مجلة كلية الشريعة والقانون، جامعة الأزهر، فرع أسيوط، ع٣٤، يوليو ٢٠٢٢، ج٢.
- **د. حاتم أحمد محمد بطيخ:** «تطور السياسة التشريعية في مجال مكافحة جرائم تقنية المعلومات (دراسة تحليلية مقارنة)»، مجلة الدراسات القانونية والاقتصادية ع٧، ج١، ٢٠٢١.
- **د. حسام محمد السيد:** المواجهة الجنائية لظاهرة الثأر الإباحي، دراسة مقارنة بين النظامين الأنجلو أمريكي واللاتيني، ج١، مجلة الدراسات القانونية والاقتصادية، جامعة السادات، مج٥، ع٢، ٢٠١٩.
- **د. حسن حماد حميد:** جريمة الابتزاز الإلكتروني، دراسة مقارنة، مجلة دراسات البصرة، العدد ٤٢، ٢٠٢١.
- **د. رامي متولي القاضي:** نحو إقرار قواعد للمسئولية الجنائية والعقاب على إساءة استخدام تطبيقات الذكاء الاصطناعي بحث مقدم إلى مؤتمر الجوانب القانونية والاقتصادية للذكاء الاصطناعي وتكنولوجيا المعلومات، كلية الحقوق جامعه المنصورة.
- **د. رزق سعد:** الحماية الجنائية للبيانات الشخصية المعالجة إلكترونيًّا في ضوء القانون رقم ١٥١ لسنه ٢٠٢٠، ورقة بحثية مقدمة للمؤتمر العلمي الدولي «الحماية القانونية للإنسان في ضوء التقدم الطبي والتكنولوجي»، كلية الحقوق جامعة السادات، ٢٠٢٢.

- **د. سعـاد شاهـين:** تكنولوجيـا الفئـات الخاصة فـي الثـورات الصناعية، مجلة الجمعية المصرية للكمبيوتر التعليمي، المجلد العاشر، ع٢، ديسمبر ٢٠٢٢.
- **د. سومية عكور:** الجرائم المعلوماتية وطرق مواجهتها بحث مقدم للملتقى العلمي لكليـة العلـوم الاستراتيجية، عمان، الأردن، المعنون بـ (الجرائم المستحدثة في ظل المتغيرات والتحولات الإقليمية) من ٢-٢٠١٤/٩/٤.
- **د. شريـف نصر أحمد:** الجوانـب الموضوعية لجرائم الدخـول غير المشروع إلى الأنظمة المعلوماتية، مجلة كلية الشريعة والقانون، ع٣٥، ج٢، ٢٠٢٢.
- **د. صالـح عبد الكريم:** المسئولية الجنائية للناشر الإلكتروني على مواقع التواصل الاجتماعي، مجلة القرطاس، ع١٧ لسنه ٢٠٢٢.
- **د. فريـدة بن عثمان:** الذكاء الاصطناعي مقاربـة قانونية، مجلة دفاتر السياسة والقانون، مجلد ١٢، ع٢، ٢٠٢٠.
- **د. كريمـة غديـري:** التزييـف العميق، نشـأة التقنيـة وتأثيرها، مجلـة الرسالة للدراسات الإعلامية، المجلد ٥، ع٤، ديسمبر ٢٠٢١.
- **د. محمـد أحمد سليمـان عيسى:** الجهـود الدوليـة الإقليمية لمواجهـة الجرائم الإلكترونية، مجلة العلوم القانونية، جامعة عجمان، الإمارات، ع ٨، يوليو ٢٠١٨.
- **د. محمد بـن عائض:** الشائعات في وسائل التواصـل الاجتماعي، مجلة الشمال للعلوم الإنسانية، مجلد٤، ع١، ٢٠١٩.
- **د. محمـد بـن عبد العزيـز المبارك:** قاعـدة (درء المفاسد على جلـب المصالح) بحـث مقدم لمؤتمر القواعد الفقهية على المسائل الطبية، المديرية العامة للشؤون الصحية بالرياض، ١٤٢٨هـ .
- **د. محمـد حسـن عبـد الله علـي:** النظـام القانوني لحمايـة البيانـات المعالجة إلكترونيًّا، دراسـة تحليلية مقارنة في ضوء اللائحة الأوروبية وبعض التشريعات ذات العلاقة، مجلة العلوم القانونية، جامعة عجمان، الإمارات، ع١٤، يوليو٢٠٢١.
- **د. محمد راشد مانع العجمي:** المسئولية الجنائية للشخص المعنوي، مجلة البحوث الفقهية والقانونية، ع٣٧، إبريل ٢٠٢٢.

- **د. محمد سعيد عبد العاطي ومحمد أحمد المنشاوي:** دور القانون الجنائي في حماية الطفل من الابتزاز الإلكتروني، مجلة البحوث الفقهية والقانونية، كلية الشريعة والقانون بدمنهور، ع٣٦، أكتوبر ٢٠٢١.
- **د. محمد محمد عبد اللطيف:** المسئولية عن الذكاء الاصطناعي بين القانون الخاص والعام، بحث مقدم إلى مؤتمر الجوانب القانونية والاقتصادية للذكاء الاصطناعي وتكنولوجيا المعلومات، كلية الحقوق -جامعة المنصورة، ٢٣-٢٤ مايو ٢٠٢١.
- **د. محمود رجب فتح الله:** الأدلة الجنائية في جرائم الابتزاز الإلكتروني، مجلة الدراسات القانونية والاقتصادية، جامعة السادات، المجلد ٨، ع٢، يونيو ٢٠٢٢.
- **د. محمود سلامة الشريف:** الطبيعة القانونية للتنبؤ بالجريمة، المجلة العربية للعلوم الأدلة الجنائية والطب الشرعي مجلد ٣، عدد٢، سنه ٢٠٢١.
- **د. محمود سلامه عبد المنعم:** جريمة الانتقام الإباحي عبر تقنية التزييف العميق المسؤولية الجنائية عنها، المجلد٢، ع ٢، ٢٠٢٢.
- **د. محمود عبد الغني جاد المولى:** الاتجاهات الحديثة في المسئولية الجنائية للكيانات التي تعمل بتقنيات الذكاء الاصطناعي، مجلة البحوث القانونية والاقتصادية، جامعة المنوفية، المجلد ٥٣، ع٣، مايو ٢٠٢١،
- **د. مصطفى صلاح عبد الحميد:** التزييف الرقمي وأثره على حجية الأدلة الرقمية في الدعاوي الجنائية دراسة فقهية مقارنة، مجلة الشريعة والقانون، القاهرة، جامعه الأزهر، ع٤٠، أكتوبر ٢٠٢٢.
- **د. معاذ الملا:** الأبعاد التاريخية لتطوّر نظرية المسؤولية الجزائية وجدلية تطبيقها في عصر الذكاء الاصطناعي: دراسة تحليلية واستشرافية، ع١٠، الجزء الأول ملحق خاص، سبتمبر٢٠٢١.
- **د. ممدوح حسن العدوان:** المسئولية الجنائية عن أفعال كيانات الذكاء الاصطناعي غير المشروعة، مجلة دراسات لعلوم الشريعة والقانون، الجامعة الأردنية، المجلد ٤٨، عدد ٤، ٢٠٢١.

- **د. نبيـل لحمر:** الأخبار الكاذبة عـبر شبكات التواصل الاجتماعـي وآثارها على اتجاهـات الـرأي العام، دراسة فـي المفهوم والعلاقة، مجلـة الباحث للدراسات الأكاديمية، المجلد ٧، ع ٢، ٢٠٢٠.
- **د. هبـه بدر أحمد:** الحمايـة الإجرائية من الشائعات «دراسـة تحليلية مقارنة»، مجلة كلية الشريعة والقانون بتفهنا، ع٢٣، لسنه ٢٠٢١.
- **د. وفـاء صقر:** المسئولية الجنائية عن الـذكاء الاصطناعي، مجلة روح القوانين، ع ٩٦، أكتوبر ٢٠٢١.
- **د. وفاء محمد أبو المعاطي صقر:** المسئولية الجنائية عن بث الشائعات عبر مواقع التواصل الاجتماعي، مجلة روح القوانين، ع٩٣، يناير ٢٠٢١.
- **د. وليد سعد الدين محمد سعيد:** المسئولية الجنائية الناشئة عن تطبيقات الذكاء الاصطناعي، مجلة العلوم القانونية والاقتصادية، جامعة عين شمس ع٢، س٣٤، يوليو٢٠٢٢.
- **د. ياسـر محمد اللمعي:** الحماية الجنائية من التضليل الإعلامي أثناء الحملات الانتخابيـة في ضوء السياسـة الجنائية التشريعية، دراسـة مقارنة مع التشريع المصري والقطري، المجلـة الدولية للقانون، كلية القانون، جامعة قطر، المجلد٩، ع٣، ٢٠٢٠.
- **د. ياسـر محمـد اللمعـي:** السياسـة الجنائية المعاصـرة في حمايـة خصوصية البيانـات الشخصيـة الإلكترونيـة، مجلـة روح القوانـين، كلية الحقـوق، جامعة طنطا، أغسطس ٢٠٢١.

ج) الرسائل العلمية:

- **أ. أحمـد محمود عواد الوقاد:** المساهمة الجنائية للقتل بالسم، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، ٢٠١٤.
- **د. أنور محمد السيد خلـف:** الحماية الجنائية للتصويت في الانتخابات، دراسة مقارنة، رسالة دكتوراه، جامعة طنطا، ٢٠٢٠.
- **أ. جوارحي عبد الستار:** جرائم الحاسوب-دراسة مقارنة بين الشريعة الإسلامية

والقانون الجزائري، رسالة ماجستير؛ كلية العلوم الاجتماعية والإنسانية، جامعة الشهيد حمة لخضر، ٢٠١٥.

- **د. خالد رمضان عبد العال:** المسئولية الجنائية عن جرائم الصحافة، دراسة مقارنة، رسالة دكتوراه، كلية الحقوق، جامعة حلوان، ٢٠٠٢.
- **أ. سارة محمد حنش:** المسؤولية الجزائية عن التهديد عبر الوسائل الإلكترونية، دراسة مقارنة، رسالة ماجستير، كلية الحقوق، جامعة الشرق الأوسط، ٢٠٢٠.
- **أ. صابر الهدام:** القانون في مواجهة الذكاء الاصطناعي، رسالة ماستر، كلية العلوم القانونية والاقتصادية والاجتماعية، جامعة سيدي محمد بن عبد الله، ٢٠٢٢.
- **أ. طه حازم الصفدي:** المسؤولية الجزائية عن إساءة استخدام وسائل التواصل الاجتماعي (دراسة تحليلية مقارنة في ضوء الأنظمة القانونية المعاصرة والشريعة الإسلامية)، رسالة ماجستير، كلية الشريعة الإسلامية، الجامعة الإسلامية بغزة، ٢٠١٩.
- **أ. عبد المجيد مازن:** استخدامات الذكاء الاصطناعي في الهندسة الكهربائية، دراسة مقارنة، رسالة ماجستير، الأكاديمية العربية، ٢٠٠٩.
- **أ. عمري موسي و يس بلال:** الآثار القانونية المترتبة عن استخدام الذكاء الاصطناعي، رسالة ماجستير، كلية الحقوق والعلوم السياسية، جامعة زيان عاشور، ٢٠٢٠.
- **د. محمد علي سويلم:** تكييف الواقعة الإجرامية، رسالة دكتوراه، جامعة عين شمس، ١٩٩٩.
- **د. محمود أحمد طه:** مبدأ شخصية العقوبات، رسالة دكتوراه، كلية الحقوق، جامعة عين شمس، ١٩٩٠.
- **أ. مروة فرج:** القتل الرحيم بين الشريعة والقانون الوضعي، رسالة ماستر، جامعة الشهيد حمة لخضر، ٢٠١٨.

ثانيًا - أهم المراجع القانونية الأجنبية:

أهم المراجع باللغة الإنجليزية:

- A Coleman: 'Deepfake app causes fraud and privacy fears in China' (BBC, 4 September 2019)
- Ad J. W. van de Gevel and Charles N. Noussair: The Nexus Between Artificial Intelligence and Economics, published by Springer, download from https://link.springer.com, 2013.
- Adomi, Esharenana: Security and Software for Cybercafesi- information science reference,2008,
- Ally Foster: Picture Reveals Sickening Online Secret, NEWS.COM.AU -JUNE 30, 2018
- Andrew Murray:Information Technology Law: The Law and Society-Fourth Edition-Oxford University Press- 2019
- Anna Yamaoka-Enkerlin: DISRUPTING DISINFORMATION: DEEPFAKES AND THE LAW LEGISLATION AND PUBLIC POLICY Vol. 22
- Avi Gesser, Megan Bannigan, Christopher Ford, Anna Gressel and Scott Caravello. «Debevoise Discusses Malicious Corporate Deepfakes». Newstex Blogs CLS Blue Sky Blog, February 1, 2023 Wednesday. advance.lexis.com/api/document?collection=news&id=urn:contentItem:67FM-9D11-F03R-N3NT-0000000-&context=1516831. Accessed February 14, 2023.
- Betül Çolak: Legal Issues of Deepfakes- January 19, 2021
- Calo, R: Artificial Intelligence Policy, A Primer and Roadmap, University of California Davis Law Review, 2017, vol. 51,
- CE Noticias Financieras English: «Reality VS fake news and deep fakes created by artificial intelligence». February 6, 2023 Monday. advance.lexis.com/api/document?collection=news&id=urn:contentItem: 67GW-R3M1-JCG7-00-00000-8117&context=151683. Accessed February 14, 2023.
- Claire Wardle & Hossein Derakhshan, Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking 20, Council of Europe DGI (2017)09 (Sept. 27, 2017), https://rm.coe.int/information-disorder-report-novem ber-20171680764666/

- Clare McGlynn, Erika Rackley, and Ruth Houghton, «Beyond 'Revenge Porn': The Continuum of Image-Based Sexual Abuse,» Feminist Legal Studies 25, no. 1 (April 1, 2017): 25–46, https://doi.org/10.1007/s106912-9343-017-
- Damon Beres: Pornhub Continued to Host 'Deepfake' Porn with Millions of Views, Despite Promise to Ban, MASHABLE (Feb. 12, 2018), https://mashable.com /201812/02//pornhub-deepfakes-ban-not-working/#cO19rvp..PqM.
- Davey Gibian: Hacking artificial intelligence: a leader's guide from deepfakes to breaking deep learning, Rowman & Littlefield, 2022
- David Greene: We Don't Need New Laws for Faked Videos, We Already Have Them, ELECTRONIC FRONTIER FOUND. https://www.eff.org/deeplinks/
- Dayani, R.; Chhabra, N.; Kadian, T., & Kaushal, R.: An Exploration of Twitter Role in Rumor Propagation Among Undergraduates, Community. In Proceedings of the 20 th international conference on World Wide Web. 2016
- Dirk Helbing: Towards Digital Enlightenment Essays on the Dark and Light Sides of the Digital Revolution, Springer Nature, 2019
- Edvinas Meskys, Julija Kalpokiene, Aidas Liaudanskas Dr. Paulius Jurcys: Regulating Deep-Fakes: Legal and Ethical Considerations.
- Elizabeth Caldera: ««Reject the Evidence of Your Eyes and Ears»: Deepfakes and the Law of Virtual Replicants,» *Seton Hall Law Review*: Vol. 50: Iss. 1, Article 5. 2019 Available at: https://scholarship.shu.edu/shlr/vol50/iss15/ p183
- Elizabeth Caldera: REJECT THE EVIDENCE OF YOUR EYES AND EARS»1: DEEPFAKES AND THE LAW OF VIRTUAL REPLICANTS, SETON HALL LAW REVIEW [Vol. 50:177]
- European Parliamentary Research Service Scientific: Tackling deepfakes in European policy- STUDY Panel for the Future of Science and Technology EPRS | Foresight Unit (STOA) PE 690.039 – July 2021,
- Felix T. Wu: Collateral Censorship and the Limits of Intermediary Immunity, 87 NOTRE DAME L. REV. 293,2013.
- Floridi Luciano: Artificial Intelligence, Deepfakes and the Future of Ectypes, Philos. Technol31, 2018. P320
- Franklin Foer: The Era of Fake Video Begins The digital manipulation of video may make the current era of «fake news» seem quaint. May 2018

- Franks (M.-A.): «‹Revenge Porn' Reform: A View from the Front Lines,» Florida Law Review, Vol. 69, 2017,
- Henry Ajder: «Deepfake Threat Intelligence: a statistics snapshot from June 2020,» Sensity, July 3, 2020: https://sensity.ai/deepfake-threat-intelligence-astatistics-snapshot-from-june-2020
- HENRY CAMPBELL BLACK: BLACK'S LAW DICTIONARY, FOURTH EDITION, THE PUBLISHER'S EDITORIAL STAFF, WEST PUBLISHING CO., 1968.
- Hin-Yan Liu,Andrew Mazibrade:Artificial Intelligence affordance :Deep Fakes as Exemplars of AI Challenges to Criminal Justice Systems,2020,United Nations Interregional Crime and Justice Research Institute ,2020,
- Huang, Y. L., Starbird, K., Orand, M., Stanek, S. A., & Pedersen, H. T.: Connected Through Crisis: Emotional Proximity and the Spread of Misinformation Online, In Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing. February 2015,.
- Husrev Taha Sencar, Luisa Verdoliva, Nasir Memon: Multimedia Forensics, 2022,Springer, Ian Goodfellow, Yoshua Bengio, Aaron Courville: Deep Learning [draft of March 30, 2015]- MIT Press- 2016
- IVAN MEHTA: A new study says nearly 96% of deepfake videos are porn. Oct 7, 2019. Available at: https://thenextweb.com/apps/201907/10//a-new-study-saysnearly-96-of-deepfake-v
- James J. F. Forest: Digital Influence Warfare in the Age of social media (Praeger Security International), Praeger Publishers Inc, 2021
- Jane Lytvynenko: «A Belgian Political Party Is Circulating A Trump Deepfake Video,» BuzzFeed News, May 20, 2018: https://www.buzzfeednews.com/article/janelytvynenko/a-belgian-political-party-just-published-a-deepfakevideo.
- Jiang, M., Cui, P., & Faloutsos, C.: Suspicious Behavior Detection: Current Trends and Future Directions, IEEE Intelligent Systems, 2016, 31(1)
- John McCarthy : 'JFK' finally recites his last speech – 55 years after his death – thanks to AI https://www.thedrum.com/news/201816/03//jfk-finally-recites-his-last-speech-55-years-after-his-death-thanks-ai

- Johnson Phylis, Punnett Ian: Redefining Journalism in an Age of Technological Advancements,IGI GLOBAL
- Joseph Migga Kizza: Ethical and Social Issues in the Information Age, Sixth Edition, Springer International Publishing AG, 2017
- Julie B. Wiest: Theorizing Criminality and Policing in the Digital Media Age, emrald,2021,
- KOENIG Gaspard:«Les «deep fakes» ou la fin du débat démocratique», Les Échos, Éditos & Analyses, 16 octobre 2019: https://www.lesechos.fr/ideesdebats/editos-analyses/les-deep-fakes-ou-la-fin-du-debat-democratique1140377
- L He et al: 'New Chinese 'deepfake' face app backpedals after privacy backlash' (CNN Business, 3 September 2019)
- Loveleen Gaur: DeepFakes Creation, Detection, and Impact, CRC Press, 2023
- Lyu, S. Detecting: deepfake videos in the blink of an eye, 29 August 2018 http://theconversation.com/detecting-deepfake-videosin-the-blink-of-aneye-101072
- Mahdi Khosravy, Isao Echizen, Noboru Babaguchi: Frontiers in Fake Media Generation and Detection, Springer, 2022,
- Manheim, K. , Kaplan, L: Artificial Intelligence: Risks to Privacy and Democracy, 2019
- Maryam Taeb, Hongmei Chi :Comparison of Deepfake Detection Techniques through Deep Learning. J. Cybersecur. Priv. 2022,
- Michael Filimowicz: Deep Fakes Algorithms and Society, Routledge, 2022
- Micheal Lanham: From Autoencoders and Adversarial Networks to Deepfakes, Apress, Year: 2021,
- Mika Westerlund, «The Emergence of Deepfake Technology: A Review,» Technology Innovation Management Review 9, no. 11 -November 2019:
- Nisha Dhanraj Dewani, Zubair Ahmed Khan, Aarushi Agarwal ,Mamta Sharma, Shaharyar Asaf Khan : Handbook of Research on Cyber Law, Data Protection, and Privacy (Advances in Information Security, Privacy, and Ethics) Information Science Reference, 2022

- Noah Giansiracusa: How Algorithms Create and Prevent Fake News: Exploring the Impacts of Social Media, Deepfakes, GPT-3, and More, r, Apress Media, 2021,
- Rudat: A. Twitter Spreads Rumors: Influencing Factors on Twitter's Role in Rumor Spread Among University Students, PhD Thesis, Tubingen: Tubingen. 2015
- Russell S. J., & Norvig: P., Artificial Intelligence, A Modern Approach, Pearson Education Limited, 3rd edition, 2014,
- Russell, S. J. , Norvig, P:, Artificial Intelligence: A Modern Approach (2nd ed.), Upper Saddle River, New Jersey: Prentice Hall, 2003
- Sabine Gless, Emily Silver Man. Thomas WEIGEND: «If Robots cause Harm, Who is to Blame? Self-Driving Cars and Criminal Laiability», New Criminal Law Review, SSRN, Janury 29, 2016
- Sales, Jonathan S., and Jessica A. Magaldi. «Deconstructing the Statutory Landscape of'Revenge Porn': An Evaluation of the Elements That Make an Effective Nonconsensual Pornography Statute.» Am. Crim. L. Rev. 57 (2020(.
- Samantha Cole: Targets of Fake Porn Are at the Mercy of Big Platforms, MOTHERBOARD (Feb. 5, 2018), https://motherboard.vice.com/en_us/article/59kzx3/targets-of-fake-porn-deepfakes-are-at-the-mercy-of-big-platform
- Sara Ashley O'Brien: Deepfakes Are Coming. Is Big Tech Ready?, CNN BUS. (Aug. 8, 2018, 11:16 AM), https://money.cnn.com/201808/08//technology/deepfakes-countermeas ures-facebook-twitter-youtube/index.html
- Sarah Sanders: «We Stand by Our Decision to Revoke This Individual's Hard Pass. We Will Not Tolerate the Inappropriate Behavior Clearly Documented in This Video,» Twitter, accessed December 8, 2022, https://twitter.com/PressSec/status/1060374680991883265Top of Form
- Shankar Bhawani Dayal , Brett van Niekerk : Deepfake Video Detection ,ECCWS 2021 20th European Conference on Cyber Warfare and Security,
- Sinduja Rangarajan: WhatsApp Is a Petri Dish of Coronavirus Misinformation, MOTHER JONESHttps://www.motherjones.com/media/202003//whats app-
- Stephen Davies: Deepfakes are the evolution of fake news and are equally as dangerous: https://www.stedavies.com/deepfakes

- Stuart J. Russell and Peter Norvig: Artificial Intelligence A Modern Approach, by A Simon & Schuster Company, 1995.
- Taylor Hatmaker: Facebook Flags Biden Video from Trump's Social Media Director as 'Partly False,' TECHCRUNCH https://tech crunch.com/202009/03// facebook-biden-video-twitter-trump/.
- Thanh Thi Nguyena, Quoc Viet Hung Nguyenb, Dung Tien Nguyena, Duc Thanh Nguyena, Thien Huynh-Thec , Saeid Nahavandid, Thanh Tam Nguyene , Quoc-Viet Phamf , Cuong M. Nguyen: Deep Learning for Deepfakes Creation and Detection: A Survey.
- Vosoughi, Soroush, Deb Roy, and Sinan Aral: «The spread of true and false news online.» science 359.6380 -2018:
- Wisskirchen, G: IBA Global Employment Institute Artificial Intelligence and Robotics and their Impact on the Workplace, 2017,
- Wooldridge M, Jennings, N. R: Intelligent Agents: Theory and Practice, The Knowledge Engineering Review, vol. 10, n°2, June 1995
- YAMAOKA-ENKERLIN: Anna. Disrupting disinformation: Deepfakes and the Law. NYUJ Legis. & Pub. Pol'y, 2019

أهم المراجع باللغة الفرنسية:

- A.Batteur: De la protection du corps à la protection de l'être humain, petites affiches, 14 décembre 1994,.
- Claire Langlais-Fontaine: Démêler le vrai du faux: étude de la capacité du droit actuel à lutter contre les deepfakes, La Revue des droits de l'homme, N°18 | 2020.
- D.Bourg: Sujet-Personne-individu-Droits, 1991, n°13, Biologie, personne et droit, P.U.F, 1991.
- Delphine Baize: De la contrefaçon à l'imitation, revue française de gestion, juin-juillet-aout 1999,
- El Kaakour, N: L'intelligence artificielle et la responsabilité civile délictuelle, Université Libanaise, Faculté de droit et des sciences politiques et administratives filière francophone, 2017,
- Jean-Nicolas ROBIN: La matière pénale à l'épreuve du numérique, THÈSE

PRÉSENTÉE POUR OBTENIR LE GRADE DE DOCTEUR, UNIVERSITÉ DE RENNES, 2017,

- L.Becker: Les limites du concept d'être humain, Cahier STS (Science – Technologie- Société(, n°11, Éthique et biologie, Ed, du Commission nationale de déontologie de la sécurité, 1986,.
- Sabrina Laroche : Les médias sociaux, nouveau canal d'influence dans la stratégie relationnelle desmarques , Université de Strasbourg , Institut d'Etudes Politiques de Strasbourg , Mémoire ,JUIN 2012
- Stéphane Detraz: Les nouvelles dispositions réprimant les atteintes à l'intimité sexuelle : faire compliqué quand on peut faire simple (Commentaire de l'article 2261-2- du code pénal issu de la loi n° 20161321- du 7 octobre 2016) Revue de science criminelle et de droit pénal comparé 20164/ (N° 4)
- Valère Ndior: Le réseau social: essai d'identification et de qualification_Droit et réseaux sociaux