كلية الشريعة والقانون بدمنهور

جامعة الأزهـر

مـجلة البحوث الفقهية والقانونية

مجلة علمية محكمّة
تصدرها كلية الشريعة والقانون بدمنهور

بحث مستل من

العدد الثامن والأربعين ـ "إصدار يناير ٢٠٢٥م ـ ١٤٤٦هـ"

الجوانب القانونية للتزييف العميق

Legal Aspects of Deepfake

الدكتـــورة

رباب مصطفى عبد المنعم الحكيم

أستاذ القانون الجنائي المساعد

كلية الدراسات الإسلامية والعربية بنات القاهرة

جامعة الأزهر

مجلـة البحـوث الفقهيــة والقانونيــة
مجلة علمية عالمية متخصصة ومُحكمة
من السادة أعضاء اللجنة العلمية الدائمة والقارئة
في كافة التخصصات والأقسام العلمية بجامعة الأزهر

المجلة مدرجة في الكشاف العربي للإستشهادات المرجعية ARABIC CITATION INDEX
على Clarivate Web of Science
المجلة مكشّفة في قاعدة معلومات العلوم الإسلامية والقانونية من ضمن قواعد بيانات دار المنظومة
المجلة حاصلة على تقييم ٧ من ٧ من المجلس الأعلى للجامعات
المجلة حاصلة على المرتبة الأولى على المستوى العربي في تخصص الدراسات الإسلامية
وتصنيف Q2 في تخصص القانون حسب تقييم معامل "ارسيف Arcif" العالمية
المجلة حاصلة على تقييم ٨ من المكتبة الرقمية لجامعة الأزهر

رقم الإيداع
٦٣٥٩

الترقيم الدولي
(ISSN-P): (1110-3779) - (ISSN-O): (2636-2805)

للتواصل مع المجلة
+201221067852
journal.sha.law.dam@azhar.edu.eg

موقع المجلة على بنك المعرفة المصري
https://jlr.journals.ekb.eg

التاريخ: 2024/10/20

الرقم: L24/0260 ARCIF

سعادة أ. د. رئيس تحرير مجلة البحوث الفقهية و القانونية المحترم

جامعة الأزهر، كلية الشريعة و القانون، دمنهور، مصر

تحية طيبة وبعد،،،

يسر **معامل التأثير والاستشهادات المرجعية للمجلات العلمية العربية (ارسيف – ARCIF)**، أحد مبادرات قاعدة بيانات "**معرفة**" للإنتاج والمحتوى العلمي، إعلامكم بأنه قد **أطلق التقرير السنوي التاسع للمجلات للعام 2024.**

يخضع معامل التأثير "ارسيف Arcif" لإشراف "مجلس الإشراف والتنسيق" الذي يتكون من ممثلين لعدة جهات عربية ودولية: (مكتب اليونيسكو الإقليمي للتربية في الدول العربية ببيروت، لجنة الأمم المتحدة لغرب آسيا (الإسكوا)، مكتبة الاسكندرية، قاعدة بيانات معرفة). بالإضافة للجنة علمية من خبراء وأكاديميين ذوي سمعة علمية رائدة من عدة دول عربية وبريطانيا.

ومن الجدير بالذكر بأن معامل "**ارسيف Arcif**" قام بالعمل على فحص ودراسة بيانات ما يزيد عن (**5000**) عنوان مجلة عربية علمية أو بحثية في مختلف التخصصات، والصادرة عن أكثر من (**1500**) هيئة علمية أو بحثية في العالم العربي. ونجح منها (**1201**) مجلة علمية فقط لتكون معتمدة ضمن المعايير العالمية لمعامل "**ارسيف Arcif**" في تقرير **عام 2024.**

ويسرنا تهنئتكم وإعلامكم بأن **مجلة البحوث الفقهية و القانونية** الصادرة عن **جامعة الأزهر، كلية الشريعة و القانون، دمنهور، مصر، قد نجحت في تحقيق معايير اعتماد معامل "ارسيف Arcif"** المتوافقة مع المعايير العالمية، والتي يبلغ عددها (**32**) **معياراً**، وللاطلاع على هذه المعايير يمكنكم الدخول إلى الرابط التالي: http://e-marefa.net/arcif/criteria/

وكان **معامل "ارسيف Arcif" العام** لمجلتكم لسنة 2024 (**0.3827**). ونهنئكم بحصول المجلة على:

- **المرتبة الأولى في تخصص الدراسات الإسلامية من إجمالي عدد المجلات (103)** على المستوى العربي، مع العلم أن **متوسط معامل "ارسيف" لهذا التخصص** كان (**0.082**). كما صُنفت مجلتكم في هذا التخصص ضمن الفئة (**Q1**) وهي الفئة العليا .
- كما صُنفت مجلتكم في **تخصص القانون** من **إجمالي عدد المجلات (114)** على المستوى العربي ضمن الفئة (**Q2**) وهي الفئة الوسطى المرتفعة ، مع العلم أن **متوسط معامل "ارسيف" لهذا التخصص** كان (**0.24**).

راجين العلم أن حصول أي مجلة ما على مرتبة ضمن الأعلى (10) مجلات في **تقرير معامل "ارسيف" لعام 2024** في أي تخصص، **لا يعني حصول** المجلة بشكل تلقائي على تصنيف مرتفع كتصنيف فئة Q1 أو Q2، حيث يرتبط ذلك بإجمالي قيمة النقاط التي حصلت عليها من **المعايير الخمسة المعتمدة لتصنيف مجلات تقرير "ارسيف" (للعام 2024) إلى فئات في مختلف التخصصات**، ويمكن الاطلاع على هذه المعايير الخمسة من خلال الدخول إلى الرابط: http://e-marefa.net/arcif/

وبإمكانكم الإعلان عن هذه النتيجة سواء على موقعكم الإلكتروني، أو على مواقع التواصل الاجتماعي، وكذلك الإشارة في النسخة الورقية لمجلتكم إلى معامل "**ارسيف Arcif**" الخاص بمجلتكم.

ختاماً، في حال رغبتكم الحصول على شهادة رسمية إلكترونية خاصة بنجاحكم في معامل "**ارسيف**"، نرجو التواصل معنا مشكورين.

وتفضلوا بقبول فائق الاحترام والتقدير

أ.د. سامي الخزندار

رئيس مبادرة معامل التأثير

" ارسيف Arcif"

الجوانب القانونية للتزييف العميق

Legal Aspects of Deepfake

الدكتـــــورة

رباب مصطفى عبد المنعم الحكيم

أستاذ القانون الجنائي المساعد

كلية الدراسات الإسلامية والعربية بنات القاهرة

جامعة الأزهر

الجوانب القانونية للتزييف العميق

رباب مصطفى عبد المنعم الحكيم
قسم القانون العام (الجنائي)، كلية الدراسات الإسلامية والعربية بنات، القاهرة جامعة الأزهر الشريف، مصر.
البريد الإلكتروني: elhakemrabab@gmail.com

ملخص البحث:

يتناول هذا البحث دراسة الجوانب القانونية لتقنية التزييف العميق (Deep Fake)، التي تُعدّ واحدة من أخطر تطبيقات الذكاء الاصطناعي وأكثرها تطورًا في العصر الحديث. تمكّن هذه التقنية من إنشاء محتوى مرئي أو صوتي مزيف يظهر بمظهر حقيقي، مما يشكل تحديًا كبيرًا على الصعيد القانوني، خاصة مع انتشار تطبيقاتها السلبية التي تهدد الحقوق الفردية والجماعية.

يركز البحث على تحليل الاستخدام غير المشروع لهذه التقنية، والذي يتضمن إنشاء مقاطع أو تسجيلات مزيفة يتم فيها التلاعب بالصور أو البيانات الشخصية للأفراد دون موافقتهم، بهدف المساس بكرامتهم، أو استخدام هذه المواد المزيفة كوسيلة للابتزاز، التشهير، أو اختلاق الوقائع الكاذبة. كما يناقش البحث مدى كفاية النصوص الجنائية في القوانين القائمة، وذلك من خلال دراسة مقارنة بين التشريعات في مصر، الإمارات، سوريا، وليبيا، للكشف عن أوجه القصور والضعف في مواجهة هذا النوع من الجرائم.

اتبع البحث المنهج التحليلي المقارن لتقييم أركان جريمة التزييف العميق وتحديد العقوبات المقررة لها في النصوص الجنائية، إلى جانب تقديم توصيات تشريعية تهدف إلى سد الثغرات القانونية، سواء عبر تعديل التشريعات القائمة أو استحداث قوانين جديدة. يسعى البحث إلى تسليط الضوء على ضرورة تعزيز

الحماية القانونية للأفراد والدول من الاستخدام السلبي للتقنيات الحديثة، وضمان توازن التشريعات مع التحديات التقنية المعاصرة.

الكلمات المفتاحية: التزييف العميق؛ الجرائم الإلكترونية؛ الذكاء الاصطناعي؛ التشريعات الجنائية؛ الخصوصية الرقمية.

Legal Aspects of Deepfake

Rabab Mostafa Elhakem
Department of Criminal Law, College Of Sharia And Law, Al-Azhar University, Cairo, Egypt.
E-mail: elhakemrabab@gmail.com

Abstract:

This research addresses the legal aspects of Deepfake technology, one of the most advanced and controversial applications of artificial Intelligence. Deepfake technology enables the creation of highly realistic but fake visual and audio content by manipulating personal data such as Images and voice recordings. The study highlights the risks associated with its misuse, Including reputational harm, blackmail, defamation, and the fabrication of false evidence. It critically examines the adequacy of current criminal legislation In Egypt, the UAE, Syria, and Libya to combat these crimes. By employing a comparative analytical approach, the research evaluates the elements of the offense, prescribed penalties, and legal responses. Ultimately, It offers recommendations for legislative Improvements, aiming to strengthen legal protections against the malicious use of Deepfake technology.

Keywords: Deepfake, Cybercrime, Artificial Intelligence, Criminal Legislation, Digital Privacy.

بسم الله الرحمن الرحيم

الحمد لله رب العالمين، والصلاة والسلام على سيد المرسلين وخاتم النبيين، وعلى آله وصحبه ومن تبعه بإحسان إلى يوم الدين، أما بعد:

فقد شهد العالم في أواخر القرن الماضي تطورا كبيرا في مجال تقنية المعلومات والتكنولوجيا، حتى ساد الاعتماد عليها في جميع الجهات الرسمية وغير الرسمية، فلم يعد الفرد بمعزل عن هذه الثورة، لا سيما في ميادين تقنية المعلومات والإعلام، فيستخدمها في حياته اليومية، كما أن الحكومات تستخدمها في تسيير شئون البلاد، وتقديم الخدمات لعموم الشعب، فلم يعد هناك حاجة إلى التنقل لإتمام الإجراءات والقيام بها، بل اعتبر التقدم التكنولوجي وسيلة العالم نحو الرقي الحضاري والاقتصادي.

بيد أن انتشار هذه التقنيات أدى من جانب آخر إلى إفراز جرائم جديدة أيضا، وذلك عن طريق الاستخدام السلبي لها، لأنها كأي منتج يمكن استخدامها وسيلة لبناء المجتمعات، كما يمكن استخدمها وسيلة لهدمها، وتعد تقنية التزييف العميق (Deep fake) التي انتشرت في السنوات الأخيرة من أهم التطورات التكنولوجية التي تعتمد على الذكاء الاصطناعي، فإنها تمكن المستخدم من اصطناع مقاطع فيديو أو تسجيل مزيف يبدو وكأنه حقيقي، وذلك عن طريق جمع صور وبيانات شخصية للمجني عليه ثم التلاعب بها ومعالجتها عبر أحد تطبيقات الذكاء الاصطناعي.

وأسهم في انتشار هذه التقنية توافر أدواتها المستخدمة، حيث لا يحتاج استخدامها إلا إلى تنزيل تطبيق معين، وجمع البيانات الشخصية للمجني عليه والتي تكون غالبا متوافرة على مختلف المواقع والمنتديات الإلكترونية، وذلك بسبب التبادل الطوعي الزائد للصور ومقاطع الفيديو والتسجيلات الصوتية عن طريق المشاركة، وانتشار

الهواتف الذكية، وحينئذ لا يبقى للجاني إلا معالجتها والتلاعب بها عبر التطبيق المنزل.

أهمية البحث:

تكمن أهمية هذا البحث في معالجة أحد أهم تطبيقات الذكاء الاصطناعي التي انتشرت في الآونة الأخيرة واستخدمها بعض الأفراد في تحقيق أهدافهم غير المشروعة، والتي نتج عنها أضرار بالغة، سواء من الناحية السياسية أو الأمنية أو الاقتصادية أو الاجتماعية.

فكانت لتقنية التزييف العميق (Deep fake) آثار سيئة على النشاط السياسي نحو التأثير على الانتخابات، أو على الأمن المجتمعي وإحداث فجوة بين السلطة والشعب، كما أن لها أثرا سيئا على الاقتصاد حيث استعملها الجناة في عمليات الاحتيال والابتزاز المالي، بالإضافة إلى آثارها السلبية على الأوضاع الاجتماعية حيث استخدمها بعض المجرمين في التشهير بالضحية أو الانتقام الإباحي منه أو التشكيك في المصداقية أو نشر أخبار كاذبة والتي تؤدي إلى رفع الثقة وإحداث بلبلة بين الأفراد، كما أنه يمكن أن تستخدم هذه التقنية في اختلاق الأزمات السياسية وتوتر العلاقات بين الدول.

فالأضرار الناتجة عن الاستخدام غير المشروع لتقنية التزييف العميق لا تقتصر على الأفراد العاديين، وإنما تمتد إلى الدول والشركات والبنوك أيضا، كما تظهر أهميته في بيان مدى كفاية النصوص الجنائية الواردة في التشريعات محل البحث والتي تتمثل في التشريع المصري والإماراتي والسوري والليبي، وهل يستلزم مواجهة ذلك تدخل المشرع بالتعديل أو سن تشريع جديد أم لا؟

إشكالية البحث وأهدافه:

تتمثل إشكالية البحث في الأسئلة التي تطرحها تقنية التزييف العميق (Deep fake) واستخدامها غير المشروع، والتي يهدف هذا البحث إلى الإجابة عنها، وهذه الأسئلة هي:

١ - ماهي تقنية التزييف العميق، وما هي سماتها؟

٢- ماهي المخاطر التي تتضمنها تقنية التزييف العميق؟

٣- ما موقف الدول من سن تشريعات تنظم استخدام تقنية التزييف العميق؟

٤- ماهي أركان جريمة الاستخدام غير المشروع لتقنية التزييف العميق؟

٥- ماهي العقوبة المقررة لجريمة الاستخدام غير المشروع لتقنية التزييف العميق، وهل تقتصر العقوبة المقررة على عقوبات أصيلة أم توجد عقوبات تبعية أو تكميلية أيضا؟

٦- ما هي الظروف التي تؤدي إلى تشديد العقوبة في جريمة الاستخدام غير المشروع لتقنية التزييف أو تخفيفها أو إعفاء الجاني من العقوبة أصلا؟

منهج البحث:

المنهج المتبع لمعالجة تقنية التزييف العميق (Deep fake) واستخدامها غير المشروع في هذا البحث هو المنهج التحليلي والمقارن، وذلك بعرض النصوص الجنائية في التشريعات المصرية والإماراتية والسورية والليبية وتحليل هذه النصوص والمقارنة بينها، وذلك بهدف الوقوف على مواطن القوة والضعف في هذه التشريعات للوصول إلى النتائج والتوصيات التي تلقي الضوء على أوجه القصور والنقص بالنسبة للاستخدام غير المشروع لتقنية التزييف العميق في هذه التشريعات، وتقديم الاقتراح للمشرع عند وجود نقص أو قصور بالتدخل، إما بإصدار تشريع خاص لمواجهة هذه الجريمة أو تعديل النصوص الموجودة.

خطة البحث:

يشتمل هذا البحث على مقدمة وثلاثة مباحث وخاتمة، وذلك على النحو التالي:

المقدمة: أتناول فيها أهمية البحث وإشكاليته وأهدافه، والمنهج المتبع فيه.

المبحث الأول: ماهية التزييف العميق (Deep fake) وسماته.

المطلب الأول: ماهية التزييف العميق (Deep fake).

المطلب الثاني: سمات التزييف العميق (Deep fake).

المبحث الثاني: مخاطر التزييف العميق (Deep fake).

المطلب الأول: المخاطر السياسية والأمنية للتزييف العميق.

المطلب الثاني: المخاطر الاقتصادية والاجتماعية للتزييف العميق.

المبحث الثالث: الجوانب القانونية للتزييف العميق (Deep fake).

المطلب الأول: المواجهة التشريعية لتقنية التزييف العميق.

المطلب الثاني: أركان جريمة التزييف العميق.

المطلب الثالث: العقوبة المقررة لجريمة التزييف العميق.

الخاتمة: تشتمل على أهم النتائج والتوصيات التي تم التوصل إليها.

المبحث الأول
ماهية التزييف العميق (Deep fake) وسماته

تمهيد وتقسيم:

أدى تطور الذكاء الاصطناعي إلى إيجاد تقنية التزييف العميق (Deep fake) بحيث يتمكن الإنسان باستخدام هذه التقنية من إنشاء فيديوهات وتسجيلات ومحادثات تبدو حقيقية، ولا يتمكن من كشفه إلا المتخصصون، فيعتمد الجاني لاصطناع فيديو أو تسجيل مزيف على مجموعة من البيانات الخاصة بالمجني عليه ويقوم بمعالجتها والتلاعب بها، فيظهر في حالة الإتيان بأعمال أو أقوال لم يأت بها في الواقع، وكان أول نشأتها سنة ٢٠١٧ حيث قام بعض الأفراد باصطناع فيديو إباحي لنجمة من نجمات هوليود.

والاستخدام غير المشروع لهذه التقنية من الجرائم العابرة للحدود، فارتكابها لا يستلزم وجود الجاني في بلد المجني عليه، كما أنها تتسم بصعوبة الكشف؛ إذ لا تترك أثراً مادياً خلفها، وفي الوقت نفسه تتسم بسهولة الارتكاب، لأن انتشار تطبيقات التزييف العميق يسر الأمر، فيمكن أن يقوم بذلك أي فرد من أفراد المجتمع.

وبناء على ذلك فإن بيان ماهية التزييف العميق وذكر سماته يستوجب تقسيم هذا المبحث إلى مطلبين، وذلك على النحو التالي:

المطلب الأول: ماهية التزييف العميق (Deep fake).

المطلب الثاني: سمات التزييف العميق (Deep fake).

المطلب الأول

ماهية التزييف العميق (Deep fake)

أولا: مفهوم التزييف العميق (Deep fake):

تعددت تعريفات التزييف العميق، فعرفه البعض بأنه:" مصطلح يشير إلى المقاطع المرئية التي يتم معالجتها، أو التعديل على صورة أو صوت شخص ما في الفيديو، ليبدو حقيقيا"(١)، وعرفه الآخر بأنه:" عبارة عن نسخة متطرفة ملفقة وهمية من بيانات سمعية وبصرية تم التلاعب بها من خلال أحد تطبيقات الذكاء الاصطناعي المعدة لذلك، والذي يعني في جوهره التقول على شخص بشيء لم يقله بواسطة تقنيات تكنولوجية حديثة"(٢)، وعرفه آخرون بأنه:" عبارة عن مقاطع فيديو يتم التلاعب بها رقميا لجعلها تبدو وكأن شخصاً يقول أو يفعل شيئا بشكل واقعي"(٣).

ويعرف التزييف العميق أيضا بأنه:" تقنية تستخدم الذكاء الاصطناعي لخلق محتوى مزيف يبدو وكأنه حقيقي، عادة ما يتم استخدامها لخلق فيديوهات أو صور

---

(١) د/ أحمد مصطفى معوض محمد محرّم، استخدامات الذكاء الاصطناعي (AI)، استخدام تقنية التزييف العميق (Deep fake) في قذف الغير نموذجا دراسة فقهية مقارنة معاصرة ص ٢٥٢٨، بحث منشور في مجلة البحوث الفقهية والقانونية، جامعة الأزهر، كلية الشريعة والقانون بدمنهور، المجلد ٣٤، العدد التاسع والثلاثون، إصدار أكتوبر ١٤٤٤هـ – ٢٠٢٢م.

(٢) د/ محمود سلامة عبد المنعم الشريف، جريمة الانتقام الإباحي عبر تقنية التزييف العميق (Deep fakes) والمسؤولية الجنائية عنها ص ٣٦٩، بحث منشور في مجلة الحقوق للبحوث القانونية والاقتصادية، جامعة الإسكندرية، كلية الحقوق، العدد الأول، يوليو ٢٠٢٢.

(٣) د/ ولاء محمد محروس الناغي، د/ ياسر محمد محروس الناغي، إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق (Deep fakes) وعلاقته بالاستخدام الآمن لتلك المواقع ص ٣٩٦، بحث منشور في مجلة العلمية لبحوث الصحافة، جامعة القاهرة، كلية الإعلام، العدد الرابع والعشرون الجزء الثالث، يوليو/ ديسمبر ٢٠٢٢م.

تظهر أشخاصا أو أحداثا أو أصواتا وتعابير وجوه تم إنشاؤها بواسطة الكمبيوتر بطريقة تجعلها تبدو وكأنها حقيقة"[١]، وورد في تعريفه أيضا بأنه:" أحد أشكال توظيف تقنيات الذكاء الاصطناعي في عملية تركيب ونقل ولصق لمحتوى فيديوهات بشكل دقيق مع إعادة صياغة المحتوى من الكلام والحركات من أجل محاكاة فيديو أصيل يوازيه في الشكل العام، ويختلف عنه من حيث محتوى الموضوع والفكرة"[٢].

ومن التعريفات التي قيلت في التزييف العميق أنه: "التقنية التي تجمع بين التزييف (fakes) وتقنية الذكاء الاصطناعي (Deep Learning) المستخدمة في تكوين وإنتاج صورة أو مقطع فيديو أو صوت لشخص غُيّر وجهه أو جسده رقميا، بحيث يبدو مثل شخص آخر أو يقوم بفعل معين، كما تستخدم هذه التقنية في خلق أخبار كاذبة ومحاولة خداع الناس والتسبب بأذى للبعض"[٣].

ويظهر من هذه التعريفات أن التزييف العميق شكل من أشكال استخدام الذكاء الاصطناعي في معالجة الصور والفيديوهات والتسجيلات وتحويلها إلى فيديو جديد بحيث يبدو حقيقيا، غير أنه مزيف يخالف الواقع في الموضوع والمحتوى.

---

(١) د/ أشرف سيد أبو العلا، المواجهة الجنائية لتقنية الديب فيك (Deep fakes) ص ٤٨٧، بحث منشور في مجلة العلوم القانونية والاقتصادية، جامعة عين شمس، كلية الحقوق، المجلد ٦٦، العدد ٣، يناير ٢٠٢٤.

(٢) د/ أحمد مصطفى معوض محمد محرّم، المرجع السابق ص ٢٥٢٨.

(٣) د/ رضا إبراهيم عبد الله البيومي، الحماية القانونية من مخاطر تطبيقات التزييف العميق في الفقه الإسلامي والقانون الوضعي دراسة تحليلية مقارنة ص ٨٣١-٨٣٢، بحث منشور في مجلة روح القوانين، جامعة طنطا، كلية الحقوق، عدد خاص- المؤتمر الدولي الثامن- التكنولوجيا والقانون.

ثانيا: نشأة التزييف العميق (Deep fake):

تمت صياغة التزييف العميق (Deep fake) لأول مرة في عام ، حيث قام أحد الأشخاص بإنشاء حساب في (Reddit)، وكان يحمل الحساب اسم (Deep fake)، وقام المستخدم بإنشاء مقطع فيديو إباحي لإحدى نجمات هوليود، وبعد ذلك أزيل هذا الحساب من الموقع سالف الذكر سنة ، وفي سنة قامت شركة سامسونج بإضافة نظام في هواتفها يمكّن المستخدمين من إنشاء مقاطع مرئية باستخدام الصور الثابتة، وظهر في سنة تطبيق يمكّن المستخدم من إنشاء فيدوهات لموتى يتحركون، ويتحدثون كالأحياء[1]، ومنذ ذلك الحين إلى يومنا هذا إزداد صنع ونشر الفيويوهات والصور المزيفة عبر تقنية التزييف العميق.

وتوجد تطبيقات عديدة لمعالجة الصور والفيديوهات وتحويلها إلى مقاطع فيديو أو صور مزيفة منها: تطبيق (Fake App)، وتطبيق (Zaog) و(Deep Face Lab) و(Face Swap) و(MYHeritage) وغيرها من التطبيقات[2]، وكانت عملية التزييف العميق في أول نشأته تتسم بالتعقيد وصعوبة التنفيذ، ولكن مع انتشار مختلف التطبيقات صار الأمر سهلا وفي متناول الجميع، سواء بالنسبة للمتخصصين أو غيرهم، كما أن هذه التقنية الآن لا تحتاج إلى بيانات كثيرة، فيمكن إنتاج فيديو بصورة أو صورتين.

---

(١) د/ ولاء محمد محروس الناغي، د/ ياسر محمد محروس الناغي، المرجع السابق ص ٣٩٦، د/ أحمد مصطفى معوض محمد محرّم، المرجع السابق ص ٢٥٣٠-٢٥٣١.

(٢) د/ محمود سلامة عبد المنعم الشريف، المرجع السابق ص ٣٦٨.

وقد أسهم بشكل أو بآخر في انتشار هذه التطبيقات وإنتاج الفيديوهات والصور المزيفة تزييفا عميقا الأغراض الترفيهية لها، وإتاحة البيانات في مختلف المنصات، لاسيما الأشخاص المشهورة والعامة[١].

ثالثا: أنواع المحتوى المزيف:

يمكن استخدام التزييف العميق في إنشاء المحتوى المرئي والصوتي، ويقصد بالأول استخدام هذه التقنية في إنتاج الصور ومقاطع الفيديو، وذلك إما بتبديل الوجه وتركيب وجه شخص آخر عبر استخدام خوارزمية التشفير (Encoder) وخوارزمية فك التشفير (Decoder Algorithms)، أو التلاعب بالوجه مثل تغيير التعابير أو مزامنة الشفاة، وذلك باستخدام خوارزمية التوليد وخوارزمية التمييز(Discriminator).

أما المحتوي الصوتي فيقصد به تركيب الصوت أو تعديله، ويتم تركيب الصوت بإنتاج تسجيل مزيف لشخص يتضمن الحديث عن موضوع معين بصوت نفس الشخص، غير أنه لم يقله في الحقيقة، أما تعديل الصوت فيكون عن طريق التلاعب والتحكم في نبرات الصوت بحيث يظهر فيه حالة الشخص أو شعوره، كأن يظهره في حالة السكر أو التمسخر أو الخوف أو الحزن[٢].

رابعا: حجم استخدام التزييف العميق (Deep fake):

ورد في التقرير الذي نشره مركز المعلومات ودعم اتخاذ القرار التابع لمجلس الوزراء المصري أن العالم شهد ارتفاعا في استخدام تقنية التزييف العميق(**Deep fake**) ، حيث ارتفع محتوى التزييف العميق عبر الإنترنت بنسبة ٩٠٠ % بين عامي ٢٠١٩ و٢٠٢٠،

---

(١) د/ أحمد مصطفى معوض محمد محرّم، المرجع السابق ص ٢٥٣٢.

(٢) دليل التزييف العميق ص ١٠، الصادر عن البرنامج الوطني للذكاء الاصطناعي، الإمارات العربية المتحدة، يوليو سنة ٢٠٢١م.

وذكر أن التوقعات تشير أن النسبة في حالة إزدياد مستمر حيث يتوقع بعض الباحثين أنه بحلول ٢٠٢٤ سيتم إنشاء ٩٠ % من محتوى الإنترنت صناعيا، وورد في هذا التقرير أيضا أن في عام ٢٠٢٢ تعرض ٦٦ % من محترفي وموظفي المؤسسات والمسؤولين عن الأمن السيبراني لهجمات التزييف العميق داخل مؤسساتهم[1].

(١) الذكاء الاصطناعي ومخاطر التزييف العميق ص ٢، تقرير دوري يصدر عن مركز المعلومات ودعم اتخاذ القرار التابع لمجلس الوزراء المصري، نشر بتاريخ ٢٥ مارس ٢٠٢٣.

المطلب الثاني

سمات التزييف العميق (Deep fake)

أولا: التزييف سلوك يتعلق بالذكاء الاصطناعي:

يعد الذكاء الاصطناعي من أهم مميزات هذا العصر، وقد تعددت استعمالاته، وكان له أثر إيجابي في كثير من الشئون العامة والخاصة، غير أن استعماله لم يتوقف على النواحي الإيجابية، وإنما استغله بعض الناس لتحقيق أهدافهم الإجرامية، وقد استخدم الجناة تقنية التزييف العميق في مختلف الجرائم، سواء كانت جرائم الأموال أو الأعراض أو الجرائم المضرة بمصالح الدولة العليا[١]، وسيأتي تفصيل ذلك لاحقا.

ثانيا: التزييف سلوك يتعلق بالتعلم العميق (Deep Learning):

تتعلق هذه السمة في حقيقة الأمر بالسمة سالفة الذكر، وبيان ذلك أن القدرة على التعلم العميق مما يتميز به السلوك الذكي، فإذ كان الإنسان يعتمد في التعلم على الملاحظة والاستفادة من الأخطاء السابقة واستقراء ما هو موجود حالياً، فإن برامج الذكاء الاصطناعي يعتمد على تعلم الآلة، وذلك عن طريق إدخال مجموعة ضخمة من المعلومات والبيانات لإيجاد نظريات وخوارزميات تكون قادرة على إيجاد أساليب وطرق عالية للاستنباط عبر تحليل البيانات الواردة، ومن أهم أمثلتها التعرف على الوجه والكلام وأنظمة التعرف على اللغة الطبيعية، والرؤية الحاسوبية[٢].

---

(١) د/ أحمد محمد فتحي الخولي، المسئولية المدنية الناتجة عن الاستخدام غير المشروع لتطبيقات الذكاء الاصطناعي «الديب فيك نموذجا» ص ٢٥٣-٢٥٥، بحث منشور في مجلة البحوث الفقهية والقانونية، جامعة الأزهر، كلية الشريعة والقانون بدمنهور، المجلد ٣٣، العدد ٣٦، أكتوبر ٢٠٢١م.

(٢) د/ أحمد مصطفى معوض محمد محرّم، المرجع السابق ص ٢٥١٢، د/ أشرف سيد أبو العلا، المرجع السابق ص ٤٨٨.

ثالثا: التزييف سلوك عابر للحدود:

جريمة التزييف العميق كغيرها من الجرائم الإلكترونية تتسم بأنها عابرة للحدود، وتكتسب هذه السمة من أمرين: الأول: طبيعة الأفعال المكونة له، وذلك لأنها تعتمد على برامج عديدة ومتداخلة من خلال شبكات الحاسب الآلي وشبكات الإنترنت، والثاني: طبيعة مساسها بمصالح الدول العديدة، فلا تقتصر آثارها على الدولة التي وقعت فيها، بل قد تتعدى إلى غيرها من الدول، سواء كانت تلك الآثار سياسية أو اقتصادية أو اجتماعية أو أمنية[1].

رابعا: التزييف سلوك يعتمد على معالجة البيانات:

يعتبر تداول الصور والفيديوهات والتسجيلات الشخصية ومشاركتها وإتاحتها لجميع الأفراد مما يتميز به العصر الراهن، ولكنه في الوقت نفسه يؤدي إلى إيجاد أرض خصبة للأشخاص الذين يريدون إساءة استخدامها، حيث يقوم الجاني عبر تقنية التزييف العميق بدمج الصور أو الفيديوهات أو التسجيلات الحاصلة من المصادر المختلفة، وإنتاج فيديو أو تسجيل جديد مزيف يخالف الأول في المحتوى والموضوع، ويخالف الواقع، وبعد ذلك يشارك هذا المُنتَج مع الآخرين، بهدف تهديد المجني عليه أو التشهير به، أو إشاعة أخبار كاذبة عنه، أو غيرها من الأهداف[2].

خامسا: التزييف العميق صعب الاكتشاف:

لا يحتاج إنتاج الفيديوهات أو التسجيلات المزيفة عبر تقنية التزييف العميق إلى الأساليب والطرق التقليدية من استعمال العنف، وإنما يستلزم الحاسب الآلي وشبكة الإنترنت فقط، ولذلك يصعب اكتشافه، لأنه يتم في الفضاء الإلكتروني، فلا يترك أثرا خارجيا ماديا يمكن الاستفادة منه في ملاحقة مرتكبه وضبطه، ويضاف إلى ذلك أيضا

---

(١) د/ أحمد محمد فتحي الخولي، المرجع السابق ص ٢٥٥.

(٢) د/ أشرف سيد أبو العلا، المرجع السابق ص ٤٨٨.

أنه ذو طبيعة فنية يحتاج كشفها إلى المتخصصين، وفي الوقت نفسه يتسم بسهولة الارتكاب، حيث لا يحتاج ارتكابها إلى صفات محددة أو خبرة معينة في الجاني، بل وسيلة ارتكابها متاحة لجميع أفراد المجتمع، وذلك عن طريق تنزيل تطبيقات معينة وجمع الصور والفيديوهات والتسجيلات المتوفرة على مختلف المنتديات الإلكترونية ووسائل التواصل الاجتماعي، ومن ثم دمجها وإنتاج فيديو أو تسجيل مزيف يبدو حقيقيا، ولا يمكن كشفه لا سيما بالنسبة للأفراد العاديين[١].

(١) د/ رضا إبراهيم عبد الله البيومي، المرجع السابق ص ٨٤١-٨٤٢.

المبحث الثاني

مخاطر التزييف العميق (Deep fake)

تمهيد وتقسيم:

تعد تقنية التزييف العميق من التطبيقات التي تعتمد على الذكاء الاصطناعي، وقد أثار استخدامها السلبي قلقا كبيرا بين الأفراد والدول، لاسيما مع تطور التطبيقات الرقمية الحديثة، إذ يمكن استخدامها في التجسس واختلاق الأزمات السياسية والتأثير في الانتخابات والتلاعب بنتائجها، والاحتيال المالي، وتأليب الرأي العام وإثارة الشغب، كما أن إساءة استخدامها يؤثر على العلاقات الاجتماعية، فقد يستخدم في التشهير والانتقام من المجني عليه، أو التشكيك في واقعة أو مصداقية أمر، أو إفلات المجرمين من العقاب، وذلك عن طريق التلاعب بأدلة الإثبات.

فدراسة مخاطر تقنية التزييف العميق يستلزم تقسيم هذا المبحث إلى مطلبين، وذلك على النحو التالي:

المطلب الأول: المخاطر السياسية والأمنية للتزييف العميق.

المطلب الثاني: المخاطر الاقتصادية والاجتماعية للتزييف العميق.

المطلب الأول
المخاطر السياسية والأمنية للتزييف العميق

أولا: المخاطر السياسية للتزييف العميق (Deep fake):

يتجلى الخطر السياسي لتقنية التزييف العميق (Deep fake) في التأثير على الانتخابات، أو التلاعب بنتائجها، واختلاق الأزمات الدبلوماسية، فيقوم المستخدم بإنشاء مقاطع فيديو للقادة السياسيين تتضمن الإساءة لمخالفيهم، أو إطلاق إشاعات بهدف التأثير على العملية الانتخابية لصالح أحد الأطراف، من أمثلة ذلك نشر مقطع فيديو يظهر فيه أحد المرشحين للرئاسة الأمريكية وينتقد مصداقية الانتخابات، والسماح للقوى الأجنبية بالتأثير على مجريات العملية الانتخابية، ومن ذلك أيضا انتشار فيديو مزيف بتقنية التزييف العميق تظهر فيه رئيسة نيوزيلندا جاسيندا أرديرن في حالة تدخين الكوكايين، مع أن الفيديو الأصل لمدمنة تم تصويره سنة ٢٠١٩، ولكن قام أحد الأشخاص بتركيب وجه الرئيسة على وجه المدمنة، ومن ذلك أيضا قيام قادة الجيش بانقلاب عسكري في دولة الجابون الأفريقية سنة ٢٠١٩، حيث كان سبب ذلك نشر فيديو مزيف عبر تقنية التزييف العميق يظهر فيه الرئيس علي بونغو بعد غيابه عدة أسابيع للمرض الذي كان قد أصابه، مما أدى بقادة الجيش إلى الانقلاب عليه[1].

ومن أمثلة استغلال تقنية التزييف العميق في العمليات الانتخابية انتشار فيديو لنانسي بيلوسي المتحدثة الرسمية للبيت الأبيض تظهر خلاله وكأنها في حالة السكر، فوجهت التهمة إلى أنصار الرئيس دونالد ترامب باستخدام التزييف العميق بهدف التأثير على الانتخابات الرئاسية التي جرت عام ٢٠٢٠، وقد نشر هذا الفيديو على صفحة (Facebook Politics WatchDog) ثم على اليوتيوب وشاهده خلال أقل من

---

(١) د/ أحمد مصطفى معوض محمد محرّم، المرجع السابق ص ٢٥٣٤.

أسبوع ٢.٥ مليون شخص[١]، مما يعني مدى انتشار مثل هذه الموضوعات وتأثيرها على العملية الانتخابية.

كما أن تقنية التزييف العميق (Deep fake) قد تستخدم في اختلاق الأزمات الدبلوماسية، مما يؤدي إلى توتر العلاقات بين الدول، وذلك عن طريق صياغة محتوى يتضمن إساءة أو خطاب كراهية ضد بعض الدول بهدف تشكيل الرأي العام، أو اصطناع فيديو مزيف يظهر فيه بعض الأفراد في حالة الاعتداء على الأشخاص المنتمين إلى تلك الدولة، فيؤدي هذا إلى التأثير على علاقتها بالدولة التي تم الاعتداء على مواطنيها، كما يتم ذلك عن طريق إنشاء فيديو يستخف فيه أحد القادة بعلم دولة أخرى أو يسخر من قراراتها السياسية، أو يعلن فيها أحد القادة الحرب ضد دولة أجنبية.

وقد أظهر تقرير لمجموعة من الباحثين في جامعة أكسفورد أن ٢٥ ٪ من المحتوى السياسي الذي تم نشره حول الانتخابات الفرنسية كان مزيفا ومضللا، ولا يمت إلى الحقيقة بأية صلة[٢]، وهذا يدل على حجم استغلال تقنية التزييف العميق في العمليات الانتخابية في مختلف الدول.

ثانيا: المخاطر الأمنية للتزييف العميق (Deep fake):

تعد تقنية التزييف العميق أحظر سلاح يهدد أمن المجتمع، وذلك عن طريق نشر إشاعات أو تصريحات كاذبة ومضللة للناس، وتتعدد مظاهر الخطر الأمني لهذه التقنية، فمن أمثلة ذلك نشر فيديو لرئيس أوكرانيا فولوديمير زيلينسكي سنة ٢٠٢٢ يأمر جنوده بإلقاء أسلحتهم، والاستسلام في القتال ضد الغزو الروسي، فنشرت الحكومة

---

(١) د/ محمود سلامة عبد المنعم الشريف، المرجع السابق ص ٣٧٠، هامش رقم (٢).

(٢) د/ أحمد محمد فتحي الخولي، المرجع السابق ص ٢٥٨-٢٥٩.

الأوكرانية بيانا رسميا أوصت فيه جنودها بتوخي الحذر من الفيديوهات المفبركة بتقنية التزييف العميق، والتي تنشر في شبكات الإنترنت، وتستهدف إحداث البلبلة والتفريق في صفوف الجيش[١].

كما أن الفيديوهات والتسجيلات المزيفة بتقنية التزييف العميق قد يؤدي إلى زعزعة الاستقرار الأمني للمجتمع، وذلك عن طريق اختلاق مشاهد تتضمن اعتداء الشرطة على المواطنين، مما قد يؤدي إلى التأثير على الرأي العام، والقيام بأعمال الشغب والتحريض على استعمال العنف، أو إنشاء فيديوهات تتضمن التصريحات المسيئة للسياسيين أو القادة، والتي قد تؤدي إلى نشوب التظاهرات والشغب والتعدي على الأموال والمصالح العامة[٢].

وفي هذا الإطار كانت مخاطر التزييف العميق على الأمن القومي والعمليات الانتخابية هي محور نقاش جلسة استماع لجنة الاستخبارات بمجلس النواب الأمريكي، إذ كانت لهذه التقنية آثار سيئة على انتخابات ٢٠٢٠، وفي هذا السياق اعتبر (Marco Rubio) العضو بهذا المجلس تقنية التزييف العميق تعادل خطورة الأسلحة النووية، حيث قال: " إن تهديد الولايات المتحدة كان يتطلب حاملات طائرات وأسلحة نووية وصواريخ بعيدة المدى، أما اليوم فيتطلب ذلك التهديد استعدادات أخرى لمواجهة قدرته على الدخول إلى أنظمة الولايات المتحدة الإلكترونية وأنظمتها البنكية أو إنتاج فيديوهات مزيفة تبدو واقعية جدا قادرة على تدمير النظام الانتخابي وإضعاف البلاد داخليا"[٣].

---

(١) د/ محمود سلامة عبد المنعم الشريف، المرجع السابق ص ٣٧٠.

(٢) د/ رضا إبراهيم عبد الله البيومي، المرجع السابق ص ٨٣٨.

(٣) د/ ولاء محمد محروس الناغي، د/ ياسر محمد محروس الناغي، المرجع السابق ص ٣٩٩.

المطلب الثاني

المخاطر الاقتصادية والاجتماعية للتزييف العميق (Deep fake)

أولا: المخاطر الاقتصادية للتزييف العميق (Deep fake):

يعد استعمال تقنية التزييف العميق في الاحتيال مصدر قلق لدى أصحاب الأموال، حيث يقوم المستخدم لهذه التقنية بفبركة صوت رئيس الشركة أو صورته ومطالبة الموظف المختص بتحويل مبالغ معينة، ومن أمثلة ذلك ما تعرضت له شركة ألمانية للطاقة من احتيال حيث طالب المحتال تحويل مبلغ ٢٢٠ ألف دولار أمريكي إلى حساب معين بعد تزييف صورة موظف رفيع المستوى في تلك الشركة[١]، ومن ذلك أيضا ما تعرضت له شركة بريطانية في مارس سنة ٢٠١٩ حيث استعمل الجاني مقطعًا صوتيًّا لرئيس الفرع الأصل يطالب فيه بتحويل مبلغ ٢٤٣ ألف دولار، ولم تُكتشف العملية إلا بعد أن طلب رئيسه الحقيقي إجراء تحويل مالي آخر، إذ كان التسجيل الصوتي يبدو حقيقيا لم يشك فيه رئيس الفرع أصلا[٢].

وتظهر التقارير والأبحاث أن ٩٢ ٪ من المتخصصين والممارسين للأمن السيبراني يشعرون بالقلق من استخدام تقنية التزييف العميق في العمليات الاحتيالية، وتشير التقديرات أن ٢٦ ٪ من الشركات الصغرى و٣٨ ٪ من الشركات الكبرى تعرضت للاحتيال باستخدام هذه التقنية، وقد أدى ذلك إلى إلحاق خسائر كبيرة للشركات التي وقعت ضحية لذلك[٣].

---

(١) د/ أحمد مصطفى معوض محمد محرّم، المرجع السابق ص ٢٥٣٥.

(٢) د/ رضا إبراهيم عبد الله البيومي، المرجع السابق ص ٨٣٨.

(٣) الذكاء الاصطناعي ومخاطر التزييف العميق ص ٢، تقرير دوري يصدر عن مركز المعلومات ودعم اتخاذ القرار التابع لمجلس الوزراء، نشر بتاريخ ٢٥ مارس ٢٠٢٣.

كما تتمثل مخاطر التزييف العميق(Deep fake) في الابتزاز المالي، فيقوم المجرم بإنشاء مقطع فيديو مزيف بحيث يظهر الشخص المراد ابتزازه بحالة مخالفة للآداب، ثم يهدده ويبتزه بنشره إذا لم يدفع له المبلغ المحدد[١]، كما أن هذه التقنية يمكن استعمالها في التأثير على أسهم الشركات والبورصة، إذ قد يقوم الجاني بتزييف صور وتصريحات مديري الشركات التي يريد الإضرار بها، فيقوم بنشرها مما يؤدي إلى تنزيل أسهم هذه الشركة.

ومن صور الاستغلال المالي للتزييف العميق ما يقوم به بعض الأشخاص من نشر شائعات وأكاذيب بهدف تحقيق مصالحه الخاصة، من ذلك بيان نشرته وزارة الداخلية المصرية بتاريخ ٢٢ من يوليو سنة ٢٠٢٢ بشأن مقطع فيديو تم تداوله عبر منصات التواصل الاجتماعي، ويظهر فيه بعض الأشخاص ويزعمون انتشار تعاطي المخدرات بالأكشاك الكائنة بالطريق الدائري بمحافظة الإسماعيلية، ويطلب من المسئولين اتخاذ كافة الإجراءات اللازمة وإزالة هذه الأكشاك، فأصدرت الوزارة بيانها بعدم وجود مثل هذه الظاهرة في هذا الطريق، وأن الفيديو المنتشر مزيف، حيث كان هدف المجرمين منه إزالة الأكشاك واستغلال المساحة لمصلحتهم الخاصة[٢].

ثانيا: المخاطر الاجتماعية للتزييف العميق (Deep fake):

تتمثل المخاطر الاجتماعية للتزييف العميق في التشهير والانتقام الإباحي، حيث يقوم الجاني بإنشاء مقطع فيديو بعد حصوله على صور وفيديوهات المجني عليه من مختلف المنصات ومواقع التواصل الاجتماعي، ونشر هذا المقطع المزيف بهدف

---

(١) د/ ولاء محمد محروس الناغي، د/ ياسر محمد محروس الناغي، المرجع السابق ص ٣٩٩-٤٠٠.

(٢) د/ رضا إبراهيم عبد الله البيومي، المرجع السابق ص ٨٣٩.

النيل من الضحية وإذلاله والانتقام منه[١]، وقد يستتبع إنتاج مقاطع الفيديوهات الإباحية الابتزاز الجنسي أو المالي أيضا، حيث يطلب الجاني من الضحية لعدم نشر الفيديو إقامة علاقة جنسية غير مشروعة معها، وقد يطلب منها مبلغا ماليا[٢].

ويعتبر الانتقام الإباحي من أوسع وجوه استغلال تقنية التزييف العميق (Deep fake)، ويبين ذلك التقرير الصادر سنة ٢٠١٩ عن مؤسسة هولندية باسم (Startup Deeptrace)، وورد فيه أن إجمالي الفيديوهات المزيفة التي عثر عليها خلال ديسمبر ٢٠١٨ وأكتوبر ٢٠١٩ هو ١٤٦٧٨ فيديو، وتشكل ٩٦٪ منها فيديوهات إباحية، وقد شوهدت من قبل ١٣٤ مليون شخصٍ، مما يعني مدى انتشار هذا النوع من استخدام التزييف العميق، والخطورة الكامنة في هذه التقنية ، ومن أمثلة ذلك ما حدث لفتاة مصرية في يناير ٢٠٢٢ حيث قام أحد المجرمين بإنشاء مقطع إباحي مزيف لها بعد الحصول على صورها من مواقع التواصل الاجتماعي، فنشر هذا المقطع بين أفراد المدينة التي تعيش فيها، مما دفع بها إلى الانتحار [٣].

ومن المخاطر الاجتماعية للتزييف العميق التشكيك في المصداقية، لأن عدم قدرة الإنسان على التفرقة بين الفيديو المزيف والحقيقي، والإشاعة والحقيقة يؤثر بشكل أو آخر على جميع الفيديوهات المنتشرة على شبكة المعلومات، كما أنه يؤدي إلى إحداث بلبلة وجدل داخل المجتمع، مما يؤدي إلى فقدان الثقة في جميع ما يتم نشره على جميع المنتديات أو مواقع التواصل الاجتماعي، فيكون الإنسان حائرا وغير متأكد

---

(١) د/ أحمد محمد فتحي الخولي، المرجع السابق ص ٢٦٠.

(٢) د/ ولاء محمد محروس الناغي، د/ ياسر محمد محروس الناغي، المرجع السابق ص ٣٩٩.

(٣) د/ محمود سلامة عبد المنعم الشريف، المرجع السابق ص ٣٧٣-٣٧٤، د/ أحمد عبد الموجود أبو الحمد زكير، جريمة التزييف الإباحي العميق دراسة مقارنة ص ٢٢٢٩، بحث منشور بمجلة القانون، جامعة القاهرة، كلية الحقوق، فرع الخرطوم، المجلد ١١، العدد ٧، سنة ٢٠٢٢.

من حقيقة المحتوى المعروض، لأنه لا يوجد طرق يمكن من خلالها معرفة مدى صحة الخبر أو الفيديو وعدم التلاعب به[١].

ومما ساعد على إشاعة الأكاذيب وانتشار الفيديوهات المزيفة والتشكيك في المصداقية توافر وتعدد مواقع التواصل الاجتماعي، فيتمكن كل فرد من أفراد المجتمع من استخدامها، وفي الوقت نفسه لا يوجد تطبيق يتأكد به من مدى صحة المعلومات، ومن أمثلة ذلك نشر فيديو مزيف يظهر فيه الرئيس الأمريكي يسخر من قرارات بلجيكا السياسية، والمقطع وإن لم يكن عالي الجودة ، وذكر في نهايته:" ومن الواضح أن التغيير المناخي مزيف تماما مثل هذا المقطع"، إلا أنه أثار جدلا كثيرا على مواقع التواصل الاجتماعي[٢].

ومن المخاطر الاجتماعية لتقنية التزييف العميق (Deep fake) التلاعب بأدلة الإثبات الرقمية في القانون الجنائي، وذلك بإظهار شخص يقتل غيره أو يسرق أمواله أو يعتدي عليه بالضرب وتوجيه السب والشتم إليه في حين أنه لم يرتكب هذه الأفعال، وإنما قام غيره بتعديل الفيديو وتركيب وجهه على وجه الجاني الأصل، فيظهر كأنه من ارتكب الجريمة[٣].

وبالإضافة إلى ما سبق ذكره فإن التصريحات العنصرية وازدراء الأديان والاعتداء على خصوصيات الأفراد وحياتهم الخاصة واستغلال بياناتهم يعد أيضا من المخاطر الاجتماعية لتقنية التزييف العميق[٤]، إذ قد يترتب على سوء استعمال هذه التقنية انتشار خطاب الكراهية والتنمر وأعمال الشغب وإحداث بلبلة في المجتمع.

---

(١) د/ رضا إبراهيم عبد الله البيومي، المرجع السابق ص ٨٤٣.

(٢) د/ أحمد محمد فتحي الخولي، المرجع السابق ص ٢٥٧

(٣) د/ أحمد مصطفى معوض محمد محرّم، المرجع السابق ص ٢٥٣٥.

(٤) د/ محمود سلامة عبد المنعم الشريف، المرجع السابق ص ٣٧٣.

المبحث الثالث

الجوانب القانونية للتزييف العميق (Deep fake)

تمهيد وتقسيم:

تقنية التزييف العميق كغيرها من التطبيقات الإلكترونية والذكاء الاصطناعي لها استخدامات إيجابية وسلبية، وبديهي أن استخدامها السلبي يشكل جريمة من الجرائم، لأن فيه اعتداء على حق الأفراد في الخصوصية والكرامة، ولأنه قد يشكل خطرا كبيرا على علاقات الدولة بغيرها من الدول، أو علاقتها مع شعبها، فالاستخدام غير المشروع لهذه التقنية يشكل جريمة، يلزم لتوافرها تحقق أركانها المادية والمعنوية، إذ لا يمكن معاقبة الجاني إلا بتوافر هذه الأركان، كما يجب بيان موقف التشريعات من هذه الجريمة، وبناء على ذلك فإن دراسة موقف المشرعين من الاستخدام غير المشروع لتقنية التزييف العميق(Deep fake) وبيان أركانها والعقوبة المقررة لها يقتضي تقسيم هذا المبحث إلى ثلاثة مطالب، وذلك على النحو التالي:

المطلب الأول: المواجهة التشريعية لتقنية التزييف العميق.

المطلب الثاني: أركان جريمة التزييف العميق.

المطلب الثالث: العقوبة المقررة لجريمة التزييف العميق.

المطلب الأول

المواجهة التشريعية لتقنية التزييف العميق (Deep fake)

لم يسن حتى كتابة هذه السطور تشريعات تنظم استخدام التزييف العميق (Deep fake)، وتعاقب على استخداماته غير المشروعة إلا تشريعان: الأول، القانون الذي أصدرته ولاية فرجينيا الأمريكية بتاريخ ١ مايو ٢٠١٩، واستهدفت من إصداره تجريم نشر المواد الإباحية المزيفة من خلال التقنيات المعدة لذلك بدون موافقة ذوي الشأن بهدف الإكراه أو المضايقة أو التخويف، فجعل المشرع في هذا القانون صنع وبيع وتوزيع الصور ومقاطع الفيديو الإباحية المزيفة جنحة من الدرجة الأولى، ويعاقب عليها بالسجن لمدة تصل إلى عام وغرامة قدرها ٢٥٠٠ دولار.

أما التشريع الثاني فأصدرته ولاية تكساس الأمريكية بتاريخ ١ سبتمبر ٢٠١٩، واستهدفت من إصداره تجريم صنع وتوزيع مقاطع الفيديو المفبركة بقصد إيذاء أحد المرشحين أو التأثير أو التلاعب بنتائج الانتخابات إذا تم ذلك خلال ثلاثين يوما من الانتخابات، واعتبر المشرع الفعل جنحة من الدرجة الأولى، ويعاقب عليه بالسجن لمدة عام أو غرامة تصل إلى ٤٠٠٠ دولار[١].

ويوجد تشريع ثالث أصدرته ولاية كاليفورنيا في أكتوبر سنة ٢٠١٩، واستهدفت من إصداره منع إنشاء أو نشر أو بث محتوى مزيف يتضمن صورة أو صوت أحد المرشحين، وذلك خلال ستين يوما من الانتخابات، غير أن هذا التشريع لا يتضمن تجريم الفعل، وإنما منح المضرور حق التعويض عما لحقه من الأضرار أو ما فاته من المكاسب[٢].

---

(١) د/ أشرف سيد أبو العلا، المرجع السابق ص ٤٩١.

(٢) د/ محمود سلامة عبد المنعم الشريف، المرجع السابق ص ٢٧٧-٢٧٩.

وبالنسبة للدول العربية والإسلامية فلم تصدر هذه الدول قوانين خاصة تنظم استخدام تقنية التزييف العميق (Deep fake)، ولكن يوجد بعض المواد القانونية في القوانين الخاصة بشأن مكافحة الجرائم الإلكترونية والمعلوماتية يمكن سريانها على الاستخدامات غير المشروعة لهذه التقنية ، فمن ذلك المادتان (١٣) و(٥٢) من مرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ في شأن مكافحة الشائعات والجرائم الإلكترونية، حيث تنص المادة (١٣) على أنه:" يعاقب بالحبس والغرامة التي لا تقل عن (٥٠,٠٠٠) خمسين ألف درهم ولا تزيد على (٥٠٠,٠٠٠) خمسمائة ألف درهم، أو بإحدى هاتين العقوبتين، كل من استخدم تقنية المعلومات أو إحدى وسائل تقنية المعلومات لجمع أو حفظ أو معالجة بيانات ومعلومات شخصية للمواطنين أو المقيمين بالدولة بالمخالفة للتشريعات النافذة في الدولة"، وتنص المادة (٥٢) على أنه:"١- يعاقب بالحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن (١٠٠,٠٠٠) مائة ألف درهم ، كل من استخدم الشبكة المعلوماتية أو وسيلة من وسائل تقنية المعلومات لإذاعة أو نشر أو إعادة نشر أو تداول أو إعادة تداول أخبار أو بيانات زائفة أو تقارير أو إشاعات كاذبة أو مغرضة أو مضللة أو مغلوطة أو تخالف ما تم الإعلان عنه رسمياً، أو بث أي دعايات مثيرة من شأنها تأليب الرأي العام أو إثارته أو تكدير الأمن العام أو إلقاء الرعب بين الناس أو إلحاق الضرر بالمصلحة العامة أو بالاقتصاد الوطني أو بالنظام العام أو بالصحة العامة. ٢- وتكون العقوبة الحبس مدة لا تقل عن (٢) سنتين والغرامة التي لا تقل عن (٢٠٠,٠٠٠) مائتي ألف درهم إذا ترتب على أي من الأفعال المذكورة بالبند (١) من هذه المادة تأليب الرأي العام أو إثارته ضد إحدى سلطات الدولة أو مؤسساتها أو إذا ارتكبت بزمن الأوبئة والأزمات والطوارئ أو الكوارث.

ومن ذلك المادة (٢٦) من القانون المصري رقم (١٧٥) لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات، حيث تنص هذه المادة على أنه:" يعاقب بالحبس مدة لا تقل عن سنتين ولا تجاوز خمس سنوات، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز ثلاثمائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من تعمد 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".

كذلك القانون السوري رقم ٢٠ لسنة ٢٠٢٢ بشأن الجرائم المعلوماتية، حيث تنص المادة (٢٦) منه على أنه:" أ- يُعاقب بالحبس من ستة أشهر إلى سنة وغرامة من (١,٠٠٠,٠٠٠) ل.س مليون ليرة سورية إلى (٢,٠٠٠,٠٠٠) ل.س مليوني ليرة سورية كل من قام بمعالجة صور ثابتة أو متحركة أو محادثات أو تسجيلات صوتية عائدة لأحد الناس بوسائل تقنية المعلومات لتصبح منافية للحشمة أو الحياء وقام بإرسالها له أو للغير أو عرضها عليه أو على الغير أو هدد بنشرها عن طريق الشبكة، وتشدد العقوبة لتصبح الحبس من سنة إلى سنتين وغرامة من (٢,٠٠٠,٠٠٠) ل.س مليوني ليرة سورية إلى (٣,٠٠٠,٠٠٠) ل.س ثلاثة ملايين ليرة سورية إذا قام الفاعل بنشرها على الشبكة.

ب- يُعاقب بالحبس من سنتين إلى ثلاث سنوات وغرامة من (٣,٠٠٠,٠٠٠) ل.س ثلاثة ملايين ليرة سورية إلى (٤,٠٠٠,٠٠٠) أربعة ملايين ليرة سورية كل من هدد بالنشر أو نشر على الشبكة صوراً ثابتة أو متحركة أو محادثات أو تسجيلات صوتية منافية للحشمة أو الحياء عائدة لأحد الناس ولو حصل عليها برضاه، وتشدد العقوبة لتصبح السجن المؤقت من خمس سنوات إلى سبع سنوات وغرامة من

(٤,٠٠٠,٠٠٠) أربعة ملايين ليرة سورية إلى (٥,٠٠٠,٠٠٠) ل.س خمسة ملايين ليرة سورية إذا وقع الجرم على قاصر.

ومن التشريعات العربية التي واكبت تطورات التكنولوجيا الحديثة القانون الليبي رقم (٥) لسنة ٢٠٢٢ بشأن مكافحة الجرائم الإلكترونية، حيث يعتبر هذا القانون من التشريعات التي عالجت الاستخدام غير المشروع لتقنية التزييف العميق (Deep fake) بشكل شبه مباشر، إذ تنص المادة (٢١) من القانون سالف الذكر على أنه:" يعاقب بالحبس مدة لا تقل عن سنة كل من مزج أو ركب بغير تصريح مكتوب أو إلكتروني من صاحب الشأن صوتا أو صورة لأحد الأشخاص باستخدام شبكة المعلومات الدولية أو بأي وسيلة إلكترونية أخرى بقصد الإضرار بالآخرين ما لم يكن ذلك مسموحاً به في القوانين المنظمة لعمل الصحافة والحقوق والحريات العامة. فإذا كان المزج أو التركيب مع صور أو أصوات إباحية ونشرها عبر شبكة المعلومات الدولية أو بأي وسيلة إلكترونية أخرى تكون العقوبة السجن مدة لا تقل عن خمس سنوات".

وحديثاً اتجهت الدول إلى سن تشريعات جديدة تواكب التطورات التكنولوجية الحديثة من ذلك مشروع القانون المقدم إلى مجلس الشيوخ الأمريكي، والذي قدمه النائب الديمقراطي جوزيف موريل والنائب الجمهوري توم كين، بوصفه راعيا مشاركا للقانون، ويعتبر وفقا لهذا التشريع مشاركة الصور الإباحية المزيفة بتقنية التزييف العميق جريمة، وكان ذلك ردا على واقعة حدثت في مدرسة ثانوية بولاية نيوجيرسي، حيث قام بعض الطلاب بمشاركة صور إباحية لإحدى زميلاتهم، وكانت الصورة مفبركة عبر تقنية التزييف العميق[1]، ومن ذلك أيضا مسودة القانون المقدم إلى

---

(١) يراجع في ذلك على الرابط التالي:

البرلمان الألماني، ويتضمن هذا القانون عقوبات صارمة للاعتداءات التي تقع انتهاكا للحقوق الشخصية من خلال التزوير الرقمي[١].

---

https://www.alhurra.com/usa/2024/06/20/%D8%A3%D8%B9%D8%AF-%D8%A7%D8%AC%D8%AA%D9%85%D8%A7%D8%B9%D9%8A%D8%A9-%D9%82%D8%B5%D8%A9-%D9%81%D8%AA%D8%A7%D8%A9-%D8%AA%D8%AD%D8%A7%D8%B1%D8%A8-%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%81%D9%8A-%D8%A7%D9%84%D9%83%D9%88%D9%86%D8%BA%D8%B1%D8%B3-%D8%A7%D9%86%D8%AA%D8%B4%D8%A7%D8%B1-%D8%B5%D9%88%D8%B1-%D8%A5%D8%A8%D8%A7%D8%AD%D9%8A%D8%A9-%D9%85%D8%B2%D9%8A%D9%81%D8%A9-%D9%84%D9%87%D8%A7

(١) يراجع ذلك على الرابط التالي:

https://www.dw.com/ar/%D8%A7%D9%84%D9%82%D9%88%D8%A7%D9%86%D9%8A%D9%86-%D9%87%D9%84-%D9%87%D9%8A-%D8%A7%D9%84%D8%AD%D9%84-%D8%A7%D9%84%D8%B3%D8%AD%D8%B1%D9%8A-%D9%84%D9%85%D8%AD%D8%A7%D8%B1%D8%A8%D8%A9-%D8%AA%D9%82%D9%86%D9%8A%D8%A9-%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/a-69762980

المطلب الثاني

أركان جريمة التزييف العميق (Deep fake)

جريمة الاستخدام غير المشروع لتقنية التزييف العميق (Deep fake) كغيرها من الجرائم تتكون من ركنين، الركن المادي الذي يتمثل في الهيكل المادي الملموس للجريمة التي لا تتحقق بدونه، فيلزم أن يكون للفعل المكون للجريمة مظهر خارجي يمكن إدراكه[١]، والركن المعنوي الذي يتمثل في العلاقة النفسية التي تربط بين ماديات الجريمة والجاني، أو هو الرابطة التي تقوم بين الفعل والفاعل، فالركن المعنوي هو الوجه الباطني النفساني للنشاط الإجرامي، كما أن الوجه الخارجي هو الركن المادي[٢]، وتفصيل أركان هذه الجريمة على النحو التالي:

أولا: الركن المادي لجريمة التزييف العميق (Deep fake):

يلزم لتوافر هذا الركن أن يصدر من الجاني سلوك إيجابي أو سلبي، إذ لا يتصور تجريم التفكير في الجريمة أو التصميم لارتكابها أو التحضير لها، كما يلزم أن ينتج هذا السلوك أثرا أو نتيجة في العالم الخارجي، وبالإضافة إلى ذلك يجب أن يكون بين السلوك الإجرامي والنتيجة صلة تربطهما، وذلك بأن يكون السلوك سببا في حدوث النتيجة[٣]، وبناء على ذلك فإن الركن المادي لجريمة التزييف العميق يستوجب تناول هذه العناصر، وذلك على النحو التالي:

---

(١) د/ محمد محيي الدين عوض، القانون الجنائي مبادئه الأساسية ونظرياته العامة (دراسة مقارنة) ص ٩٧، الناشر: مطبعة جامعة القاهرة والكتاب الجامعي، سنة ١٩٨١م، د/ جاسم خريبط خلف، شرح قانون العقوبات القسم العام ص ١١١، الناشر: منشورات زين الحقوقية بيروت – لبنان، الطبعة الثالثة.

(٢) د/ محمود نجيب حسني، النظرية العامة للقصد الجنائي (دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية) ص ٩، الناشر: دار النهضة العربية، سنة ٢٠٠٦، د/ رمسيس بهنام، النظرية العامة للقانون الجنائي ٧٢٣، الناشر: منشأة المعارف بالإسكندرية، الطبعة الأولى سنة ١٩٩٩م، د/ فوزية عبد الستار، شرح قانون العقوبات القسم العام ص ٤٦٧، الناشر: دار النهضة العربية، سنة ١٩٨٧م.

(٣) د/ رمسيس بهنام، المرجع السابق ص ٤٣٢ وما بعدها، د/ أحمد شوقي عمر أبو خطوة، شرح الأحكام العام لقانون العقوبات ص ١٧٧، الناشر: دار النهضة العربية.

١ - **السلوك الإجرامي لجريمة التزييف العميق (Deep fake):**

يقصد بالسلوك الإجرامي النشاط الإرادي الذي يأتيه الجاني، والذي يشكل حركة في الجسم أو عضوا من أعضائه، أو الامتناع عنه[١]، وهذا السلوك يختلف باختلاف الجرائم، وذلك لاعتبارات متعددة نحو: طبيعته والمدة اللازمة لتنفيذه والظروف المسببة له[٢].

ويتمثل السلوك الإجرامي للاستخدام غير المشروع لتقنية التزييف العميق (**Deep fake**) في القيام بإجراءات التعديلات والتغييرات على البيانات الشخصية للمجني عليه، وذلك عن طريق مزج أو تركيب الصور أو الفيديوهات أو التسجيلات لأحد أفراد المجتمع بحيث تبدو حقيقية، ولا يتمكن من كشفها إلا المتخصصون[٣]، وقد عبر عن هذا المعنى المشرع الإماراتي بمعالجة بيانات ومعلومات شخصية للمواطنين أو المقيمين بالدولة[٤]، وعبر عنه المشرع المصري بمعالجة معطيات شخصية للغير[٥]، أما المشرع السوري فعبر عنه

---

(١) د/ إبراهيم عيد نايل، قانون العقوبات القسم العام (النظرية العامة للجريمة) ص ١٣٤ -١٣٥، الناشر: دار النهضة العربية، سنة ٢٠٢٠، د/ أحمد شوقي عمر أبو خطوة، شرح الأحكام العام لقانون العقوبات ص ١٧٨، الناشر: دار النهضة العربية.

(٢) د/ أحمد عوض بلال، مبادئ قانون العقوبات المصري القسم العام المرجع السابق ص ٢٦٣، الناشر: دار النهضة العربية، سنة ٢٠١٠.

(٣) د/ رامي متولي القاضي، شرح قانون مكافحة جرائم تقنية المعلومات رقم (١٧٥) لسنة ٢٠١٨ مقارنا بالتشريعات المقارنة والمواثيق الدولية ص ١٧٩، الناشر: مركز الدراسات العربية، الطبعة الأولى ١٤٤١هـ - ٢٠٢٠، د/ محمد على سويلم، شرح قانون جرائم تقنية المعلومات ص ٤١٥، الناشر: دار المطبوعات الجامعية، الطبعة الأولى ٢٠١٩.

(٤) ويقصد بالمعالجة وفقا للتشريع الإماراتي: إجراء أو تنفيذ عملية أو مجموعة عمليات على البيانات أو المعلومات، سواء تعلقت بأشخاص طبيعية أو اعتبارية، بما في ذلك جمع واستلام وتسجيل وتخزين وتعديل ونقل واسترجاع ومحو تلك المعلومات، يلاحظ أن التعريف لا يشتمل على تزييف البيانات، إن كان قد يدخل ضمن التعديل.

(٥) ويقصد بالمعالجة وفقا للتشريع المصري: أي عملية إلكترونية أو تقنية تتم كليا أو جزئيا لكتابة أو تجميع، أو تسجيل، أو حفظ، أو تخزين، أو دمج، أو عرض، أو إرسال، أو استقبال، أو تداول، أو نشر، أو محو، أو تغيير، أو تعديل، أو استرجاع، أو استنباط للبيانات والمعلومات الإلكترونية، ذلك

بمعالجة صور ثابتة أو متحركة أو محادثات أو تسجيلات صوتية عائدة لأحد الناس، وعلى عكس هذه التشريعات فقد عبر عنه المشرع الليبي بمزج أو تركيب صوت أحد الأشخاص أو صورته، ويعتبر هذا من أدق التعبيرات، لإفادته المعنى المقصود بصورة كاملة.

ويقصد بالبيانات والمعلومات الشخصية كما نص عليه المشرع الإماراتي في المادة الأولى من قانون رقم (٣٤) لسنة ٢٠٢١:" المعلومات أو البيانات الخاصة بالأشخاص الطبيعيين متى كانت مرتبطة بحياتهم الخاصة أو تحدد هويتهم أو يمكن من خلال ربط هذه المعلومات والبيانات بطريقة مباشرة أو غير مباشرة تحديد ومعرفة هوية الشخص"، أما المشرع المصري فلم يعرض للمقصود بالمعطيات الشخصية، وإن كان قد عرف في المادة الأولى من القانون رقم (١٧٥) لسنة ٢٠١٨ البيانات الشخصية[1] بقوله:" بيانات متعلقة بشخص طبيعي محدد أو يمكن تحديده، بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى"، إلا أنه لا يوجد في الحقيقة أي فرق بينهما، وإن كان من المستحسن التعرض لتعريفه، لاسيما وأنه قد

باستخدام أي وسيط من الوسائط أو الحاسبات أو الأجهزة الأخرى الإلكترونية أو المغناطيسية أو الضوئية أو ما يُستحدث من تقنيات أو وسائط أخرى، هذا التعريف وإن لم ينص على تزييف البيانات كالتشريع الإماراتي إلا أنه كان أكثر وضوحا، حيث تضمن عبارات الدمج والمحو والتغيير والتعديل، صور التزييف لا تخرج عن إحدى هذه العمليات.

(١) وعرف المشرع المصري البيانات الشخصية مرة أخرى بتفصيل أكثر في القانون رقم (١٥١) لسنة ٢٠٢٠ بشأن حماية البيانات الشخصية، حيث تنص الفقرة الأولى من المادة الأولى على أنه:" البيانات الشخصية: أي بيانات متعلقة بشخص طبيعي محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخري كالاسم، أو الصوت، أو الصورة، أو رقم تعريفي، أو محدد للهوية عبر الإنترنت، أو أي بيانات تحدد الهوية النفسية، أو الصحية، أو الاقتصادية، أو الثقافية، أو الاجتماعية".

خصص هذه المادة لذكر التعريفات[١].، وبناء على ذلك فإن البيانات الشخصية تشمل صورة المجني عليه وصوته وعنوان سكنه ورقم هاتفه، لأن الجاني قد يستخدم هذه البيانات في التلاعب وإجراء التغييرات والتعديلات في الصوت أو الصورة الخاصة بالضحية[٢].

وهذه البيانات قد تكون متوفرة ومتاحة، وذلك بأن يكون صاحبها قد تنازل عنها باختياره ووضعها على مختلف المواقع، وقد تكون محمية مشفرة لا يريد صاحبها إطلاع الغير عليها، وذلك بأن تكون مرفوعة على الإيميل الخاص أو أجهزة الحاسب الآلي أو الهواتف الذكية أو بنوك المعلومات نحو: شركة الاتصالات والهيئات الحكومية كهيئة البريد أو الصحة أو السجل المدني، ففي هذا النوع من البيانات لا يمكن الحصول عليها إلا عن طريق اختراق هذه الحماية[٣]، وهو ما يعتبر جريمة بذاتها وفقا للتشريع المصري[٤]،

---

(١) د/ محمود سلامة عبد المنعم الشريف، المرجع السابق ص ٤١٣.

(٢) د/ أحمد عبد الموجود أبو الحمد زكير، المرجع السابق ص ٢٢٨١.

(٣) د/ محمود سلامة عبد المنعم الشريف، المرجع السابق ص ٤٠٧-٤٠٨.

(٤) حيث تنص المادة (١٤) من القانون رقم (١٧٥) لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات على أنه: يُعاقب بالحبس مدة لا تقل عن سنة، بغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمدا، أو دخل بخطأ غير عمدي وبقى 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، غرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين"، تنص المادة (١٨) من ذات القانون على أنه:" يُعاقب بالحبس مدة لا تقل عن شهر، بغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين، كل من أتلف أو عطل أو أبطأ أو اخترق بريدًا إلكترونيًا أو موقعًا أو حسابًا خاصًا بآحاد الناس. فإذا وقعت الجريمة على بريد إلكتروني أو موقع أو حساب خاص بأحد الأشخاص الاعتبارية الخاصة، تكون العقوبة الحبس مدة لا تقل عن ستة أشهر وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز مائتي ألف جنيه، أو

والإماراتي[١]، والسوري[٢]،

بإحدى هاتين العقوبتين"، تنص المادة (٢٠) من القانون سالف الذكر على أنه:" يُعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن خمسين ألف جنيه ولا تجاوز مائتي ألف جنيه، أو بإحدى هاتين العقوبتين، كل من دخل عمدا، أو دخل بخطأ غير عمدى وبقى بدون وجه حق، أو تجاوز حدود الحق المخول له من حيث الزمان أو مستوى الدخول أو اخترق موقعا أو بريدا إلكترونيا أو حسابا خاصا أو نظاما معلوماتيا يُدار بمعرفه أو لحساب الدولة أو أحد الأشخاص الاعتبارية العامة، أو مملوكا لها أو يخصها. فإذا كان الدخول بقصد الاعتراض أو الحصول بدون وجه حق على بيانات أو معلومات حكومية، تكون العقوبة السجن، الغرامة التي لا تقل عن مائة ألف جنيه ولا تجاوز خمسمائة ألف جنيه. وفى جميع الأحوال إذا ترتب على أي من الأفعال السابقة إتلاف تلك البيانات أو المعلومات أو ذلك الموقع أو الحساب الخاص أو النظام المعلوماتي أو البريد الإلكتروني أو تدميرها أو تشويهها أو تغييرها أو تصميمها أو نسخها أو تسجيلها أو تعديل مسارها أو إعادة نشرها أو إلغاؤها كليا أو جزئياً بأي وسيلة كانت، تكون العقوبة السجن والغرامة التي لا تقل عن مليون جنيه ولا تجاوز خمسة ملايين جنيه".

(١) حيث تنص المادة الثانية من المرسوم بالقانون الاتحادي رقم (٣٤) لسنة ٢٠٢١ في شأن مكافحة الشائعات والجرائم الإلكترونية على أنه:" ١- يعاقب بالحبس والغرامة التي لا تقل عن (١٠٠,٠٠٠) مائة ألف درهم ولا تزيد على (٣٠٠,٠٠٠) ثلاثمائة ألف درهم، أو بإحدى هاتين العقوبتين، كل من اخترق موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية معلومات.

٢- وتكون العقوبة الحبس مدة لا تقل عن (٦) ستة أشهر والغرامة التي لا تقل عن (١٥٠,٠٠٠) مائة وخمسون ألف درهم ولا تزيد على (٥٠٠,٠٠٠) خمسمائة ألف درهم، أو بإحدى هاتين العقوبتين، إذا ترتب على الاختراق إحداث أضرار أو تدمير أو إيقاف عن العمل أو تعطيل موقع إلكتروني أو نظام معلومات إلكتروني أو شبكة معلومات أو وسيلة تقنية المعلومات، أو إلغاء أو حذف أو تدمير أو إفشاء أو إتلاف أو تغيير أو نسخ أو نشر أو إعادة نشر أو الحصول على أي بيانات أو معلومات أو خسارة سريتها. ٣- تكون العقوبة الحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن (٢٠٠,٠٠٠) مائتي ألف درهم ولا تزيد على (٥٠٠,٠٠٠) خمسمائة ألف درهم، أو بإحدى هاتين العقوبتين، إذا كان الاختراق بغرض الحصول على البيانات أو المعلومات لتحقيق غرض غير مشروع".

(٢) حيث تنص المادة (٢٣) من القانون رقم ٢٠ لسنة ٢٠٢٢ بشأن الجرائم المعلوماتية على أنه:" أ- يُعاقب بالحبس من شهر إلى ستة أشهر وغرامة من (٣٠٠,٠٠٠) ل.س ثلاثمئة ألف ليرة سورية

والليبي[1].

إلى (٤٠٠,٠٠٠) ل.س أربعمئة ألف ليرة سورية كل من دخل بطريقة غير مشروعة إلى نظام معلومات أو موقع إلكتروني أو حساب شخصي، تشدد العقوبة لتصبح الحبس من سنة إلى ثلاث سنوات وغرامة من (٥٠٠,٠٠٠) ل.س خمسمئة ألف ليرة سورية إلى (٧٠٠,٠٠٠) ل.س سبعمئة ألف ليرة سورية إذا وقع الدخول على نظام معلومات أو موقع إلكتروني أو حساب شخصي عائد لجهة عامة أو مصرف أو مؤسسة مالية مشتركة أو خاصة. ب- يعاقب بالحبس من سنة إلى ثلاث سنوات وغرامة من (١,٠٠٠,٠٠٠) ل.س مليون ليرة سورية إلى (٢,٠٠٠,٠٠٠) ل.س مليوني ليرة سورية إذا قام الفاعل بنسخ المعلومات التي وصل إليها، أو استخدمها، أو أفشاها، أو حذفها، أو قام بتعديلها، تشدد العقوبة لتصبح السَّجن المؤقت من خمس سنوات إلى سبع سنوات، غرامة من (٣,٠٠٠,٠٠٠) ل.س ثلاثة ملايين ليرة سورية إلى (٤,٠٠٠,٠٠٠) ل.س أربعة ملايين ليرة سورية إذا كانت المعلومات عائدة لجهة عامة أو مصرف أو مؤسسة مالية مشتركة أو خاصة. ج- يعاقب بالحبس من ثلاث سنوات إلى خمس سنوات وغرامة من (٥,٠٠٠,٠٠٠) ل.س خمسة ملايين ليرة سورية إلى (٦,٠٠٠,٠٠٠) ل.س ستة ملايين ليرة سورية إذا قام الفاعل بنسخ المعلومات التي وصل إليها وحذفها، تشدد العقوبة لتصبح السجن المؤقت من سبع سنوات إلى عشر سنوات وغرامة من (٦,٠٠٠,٠٠٠) ستة ملايين ليرة سورية إلى (٧,٠٠٠,٠٠٠) ل.س سبعة ملايين ليرة سورية إذا كانت المعلومات عائدة لجهة عامة أو مصرف أو مؤسسة مالية مشتركة أو خاصة".

(١) حيث تنص المادة (١١) من القانون رقم (٥) لسنة ٢٠٢٢ م بشأن مكافحة الجرائم الإلكترونية على أنه:" يعد الدخول لأجهزة و أنظمة الحاسب الآلي أو إلى نظام معلوماتي أو شبكة معلوماتية أو موقع إلكتروني غير مشروع، إذا تم الاختراق بشكل متعمد لوسائل وإجراءات الحماية لها بشكل كلي أو جزئي دون تصريح أو بما يخالف التصريح، تنص المادة (١٢) من ذات القانون على أنه:" يعاقب بالحبس مدة لا تزيد عن سنة أو بغرامة لا تقل عن (١٠٠) مائة دينار ولا تزيد على (٥٠٠) خمسمائة دينار أو العقوبتين معاً، كل من خالف أحكام المادة الحادية عشرة من هذا القانون. وتكون العقوبة الحبس مدة لا تقل عن سنة وبغرامة لا تقل عن (٥٠٠) خمسمائة دينار ولا تزيد على (٥,٠٠٠) خمسة آلاف دينار إذا كان الدخول بقصد إلغاء أو حذف أو إضافة أو تدمير أو إفشاء أو إتلاف أو حجب أو تعديل أو نقل أو نسخ بيانات أو تعطيل عمل نظام معلومات أو تغيير موقع إلكتروني أو إلغائه أو إتلافه أو تعديل محتوياته أو انتحال شخصية مالكه. فإذا نجم عن الدخول إعاقة عمل النظام المعلوماتي أو تعطيل الشبكة المعلوماتية أو عمل الموقع الإلكتروني أو إفساد محتوياتهم تكون العقوبة السجن والغرامة التي لا تقل عن (١٠,٠٠٠) عشرة آلاف دينار".

ويجب أن يقع السلوك الإجرامي عبر استخدام تقنية المعلومات أو البرنامج المعلوماتي أو شبكة المعلومات الدولية، ويقصد بتقنية المعلومات وفقا للتشريع الإماراتي: كل أشكال التقنية المستخدمة لإنشاء ومعالجة وتخزين وتبادل واستخدام نظم المعلومات الإلكترونية والبرامج المعلوماتية والمواقع الإلكترونية والشبكة المعلوماتية وأي وسيلة من وسائل تقنية المعلومات، والمقصود بها وفقا للتشريع المصري: أي 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 سلكيا أو لاسلكيا، وقريب من هذا تعريف المشرع السوري والذي عرفها بأنها:" الأدوات التي تُستخدم في معالجة المعلومات وتوليدها ونقلها وتبادلها وحفظها.

والمقصود بوسائل تقنية المعلومات: أي أداة إلكترونية مغناطيسية، بصرية، كهروكيميائية، أو أي أداة أخرى تستخدم لمعالجة البيانات الإلكترونية وأداء العمليات المنطقية والحسابية، أو الوظائف التخزينية، ويشمل أي وسيلة موصلة أو مرتبطة بشكل مباشر أو غير مباشر، تتيح لهذه الوسيلة تخزين المعلومات الإلكترونية أو إيصالها للآخرين، كما أن المقصود بالبرنامج المعلوماتي: مجموعة الأوامر والتعليمات المعبر عنها بأية لغة أو رمز أو إشارة، والتي تتخذ أي شكل من الأشكال، ويمكن استخدامها بطريق مباشر أو غير مباشر في حاسب آلي لأداء وظيفة أو تحقيق نتيجة سواء كانت هذه الأوامر والتعليمات في شكلها الأصل أو في أي شكل آخر تظهر فيه من خلال حاسب آلي، أو نظام معلوماتي.

والسلوك الإجرامي للاستخدام غير المشروع للتزييف العميق (Deep fake) يمر بمرحلتين: الأولى: مرحلة جمع المعلومات والبيانات، وقد سبق أن هذه البيانات قد

تكون متوفرة، وقد تكون غير متوفرة فيحصل عليها الجاني بطرق غير مشروعة مما يشكل جريمة بذاتها، فتتحقق حينئذ حالة تعدد الجرائم، وتتمثل المرحلة الثانية في اصطناع فيديو مزيف من خلال معالجة البيانات والصور والفيديوهات والتسجيلات الحاصلة سابقا بواسطة معادلات وخوارزميات الذكاء الاصطناعي والتي تقوم بإنتاج فيديو أو تسجيل خاص بالمجني عليه لا يتمكن من كشفه إلا المتخصصون[١].

ومن عناصر الركن المادي للاستخدام غير المشروع لتقنية التزييف العميق (Deep fake) أن يتم ربط البيانات التي يتم معالجتها والتلاعب بها في محتوى مناف للآداب العامة أو إظهارها بصورة تمس شرف المجني عليه واعتباره[٢] [٣]، وقد نص على ذلك

---

(١) د/ محمود سلامة عبد المنعم الشريف، المرجع السابق ص ٤٠٧-٤١٠، د/ أشرف سيد أبو العلا، المرجع السابق ص ٥٠٥.

(٢) يقصد بالآداب العامة مجموعة من القواعد الدينية والأخلاقية التي يلزم الناس بها أنفسهم في علاقاتهم الاجتماعية، يقصد بالشرف والاعتبار المكانة التي يتمتع بها الشخص في المجتمع الذي ينتمي إليه، التي تتحدد وفقا لها درجة تقدير الناس واحترامهم له، تتكون من رصيد تصرفاته وصفاته الموروثة والمكتسبة، فكرة الآداب العامة والشرف والاعتبار من الأفكار الاجتماعية التي تتغير بتغير الزمان والمكان، فما يعتبر ماسا بالآداب في مجتمع أو زمن قد لا يعتبر كذلك في مجتمع أو زمان آخر، بناء على ذلك تحدد الأفعال الماسة بالآداب العامة والشرف والاعتبار وفقاً للقيم والمعايير السائدة في المجتمع الذي ينتمي إليه المجني عليه. (د/ محمد على سويلم، المرجع السابق ص ٤١٦، د/ محمد زكي أبو عامر، الحماية الجنائية للعرض في التشريع المصري ص ٣٦، الناشر: الفنية للطباعة والنشر، سنة ١٩٨٥، د/ محمود نجيب حسني، شرح قانون العقوبات القسم الخاص ص ٦٩٥، الناشر: دار المطبوعات الجامعية، الطبعة السادسة، سنة ٢٠١٩م، د/ محمد ناجي ياقوت، فكرة الحق في السمعة ص ١٨، الناشر: منشأة المعارف بالإسكندرية جلال حزي وشركاه، دون عدد الطبع وتاريخ النشر، د/ عبد الرحمن محمد إبراهيم خلف، الحماية الجنائية للحق في الشرف دراسة تحليلية تأصيلية ص ٣٥، رسالة دكتوراه، كلية الحقوق جامعة القاهرة ١٩٩٢م).

(٣) د/ رامي متولي القاضي، المرجع السابق ص ١٨٠، د/ أحمد عبد الموجود أبو الحمد زكير، المرجع السابق ص ٢٢٨٢.

المشرع المصري والسوري، أما المشرع الليبي فلم يكتف بالنص على هذه الصورة من الاستخدام غير المشروع للتزييف العميق، وإنما ذكر نصا عاما يشمل كافة الأحوال التي يتم مزج الصور والفيديوهات والتسجيلات بقصد الإضرار بالآخرين، فيكفي وفقا لهذا التشريع أن يستهدف الجاني من استخدام تقنية التزييف العميق الإضرار بالغير، يستوي في ذلك أن يكون الضرر ماليا أو أخلاقيا، فلا يشترط أن يتم المزج والتركيب بهدف ربط البيانات بمحتوى مناف للآداب العامة والحياء العام، ولكنه اعتبر مزج الصور والتسجيلات الإباحية من الظروف المشددة، وعلى عكس هذه التشريعات اعتبر المشرع الإماراتي مجرد استخدام تقنية المعلومات أو إحدى وسائل تقنية المعلومات بهدف جمع أو حفظ أو معالجة بيانات ومعلومات شخصية للمواطنين أو المقيمين بالدولة جريمة، شريطة أن يتم ذلك بالمخالفة للتشريعات النافذة في الدولة، فلا يستلزم تحقيق الجريمة وفقا لهذا التشريع ربط البيانات بمحتوى مناف للحياء العام أو الآداب العامة، كما لا يستلزم قصد الإضرار بالآخرين.

ولم يستلزم المشرع المصري والإماراتي والليبي لوقوع هذه الجريمة مشاركة الفيديو أو التسجيل المزيف أو بثهما أو إرسالهما للغير، فالجريمة تتحقق بمجرد التلاعب بالصور والفيديوهات والتسجيلات المتعلقة بالمجني عليه، سواء نشرها أو اطلع الغير عليها أم لا، كأن يصنع فيديو لأحد الأشخاص ليحفظه لنفسه أو يستفيد منه في ملذاته الشخصية، وعلى العكس من ذلك استلزم المشرع السوري أن يقوم الجاني بمشاركة الفيديو المزيف أو التهديد بنشره، حيث تنص الفقرة الأولى من المادة (٢٦) من القانون رقم ٢٠ لسنة ٢٠٢٢ بشأن الجرائم المعلوماتية على أنه:" يُعاقب بالحبس من ستة أشهر إلى سنة وغرامة من (١,٠٠٠,٠٠٠) ل.س مليون ليرة سورية إلى (٢,٠٠٠,٠٠٠) ل.س مليوني ليرة سورية كل من قام بمعالجة صور ثابتة أو متحركة أو محادثات أو تسجيلات صوتية عائدة لأحد الناس بوسائل تقنية المعلومات لتصبح منافية للحشمة أو الحياء وقام بإرسالها له أو للغير أو عرضها عليه أو على الغير أو هدد بنشرها عن طريق الشبكة".

ولكن قد تعتبر نشر البيانات المزيفة من الظروف المشددة وفقا للتشريع الإماراتي والليبي، فقد رفع المشرع الإماراتي في المادة (٥٢) من قانون مكافحة الشائعات والجرائم الإلكترونية عقوبة الحبس إلى مدة لا تقل عن سنة والغرامة إلى مائة ألف درهم إذا استخدم الجاني استخدام الشبكة المعلوماتية أو وسيلة من وسائل تقنية المعلومات لإذاعة أو نشر أو إعادة نشر أو تداول أو إعادة تداول أخبار أو بيانات زائفة أو تقارير أو إشاعات كاذبة أو مغرضة أو مضللة أو مغلوطة أو تخالف ما تم الإعلان عنه رسميا، أو بث أي دعايات مثيرة من شأنها تأليب الرأي العام أو إثارته أو تكدير الأمن العام أو إلقاء الرعب بين الناس أو إلحاق الضرر بالمصلحة العامة أو بالاقتصاد الوطني أو بالنظام العام أو بالصحة العامة، كما أن المشرع الليبي اعتبر وفقا للفقرة الثانية من المادة (٢١) من قانون مكافحة الجرائم الإلكترونية المزج أو التركيب مع صور أو أصوات إباحية ونشرها عبر شبكة المعلومات الدولية من الظروف المشددة، فرفع العقوبة من الحبس لمدة لا تقل عن سنة إلى السجن مدة لا تقل عن خمس سنوات.

٢- **النتيجة الإجرامية**:

تعد النتيجة الإجرامية العنصر الثاني من العناصر المكونة للركن المادي، وهي الأثر المترتب على النشاط الإجرامي الذي يمكن ملاحظته من خلال التغيير الذي يحدث في العالم الخارجي[١]، وذهب جانب من الفقه إلى أن للنتيجة معنيين: المعني المادي والمعنى القانوني، فهي وفقا للمعنى المادي التغيير الملموس الذي يحدث في العالم الخارجي وتدركه الحواس نحو الموت في جرائم القتل وانتقال الحيازة في جرائم السرقة، ، سواء كان التغيير ماديا أو

(١) د/ محمد زكي أبو عامر، قانون العقوبات القسم العام ص ١١٨، الناشر: منشأة المعارف بالإسكندرية، سنة ١٩٩٣، د/ أمين مصطفى محمد، قانون العقوبات القسم العام (النظرية العامة للجريمة) ص ٢٣١، الناشر: منشورات الحلبي الحقوقية، الطبعة الأولى، سنة ٢٠١٠، د/ إبراهيم عيد نايل، المرجع السابق ص ١٤٦.

معنويا، يصيب المصلحة الخاصة، أو المصلحة العامة[١]، ويقصد بها وفقا للمدلول القانوني الاعتداء على المصلحة التي يحميها قانون العقوبات، وذلك بإهدارها كاملا أو بالانتقاص منها أو بتعرضها للخطر فقط، وبناء على ذلك يعتبر الاعتداء على الحق في الحياة أو الحق في الملكية نتيجة قانونية لجريمة القتل والسرقة[٢]، وفي الحقيقة فإن كلا المعنيين وجهان لعملة واحد، حيث إن النتيجة القانونية تحدد النموذج القانوني للجريمة، والتي يجب أن تطابقها النتيجة المادية، وإلا فلا اعتبار لها[٣].

واختلف الفقه في جريمة الاستخدام غير المشروع للتزييف العميق (Deep fake) على اتجاهين:

الاتجاه الأول: يرى جانب من الفقه وبحق أن الاستخدام غير المشروع لتقنية التزييف العميق من جرائم السلوك المادي ذي المضمون النفسي، فلا يستلزم أمرا آخر سوى معالجة البيانات الشخصية للغير، فوقوع الجريمة لا يستلزم نتيجة معينة حتى يؤدي عدم وقوعها إلى توقف النشاط في مرحلة الشروع[٤].

---

(١) د/ أحمد فتحي سرور، الوسيط في قانون العقوبات القسم العام، ص ٥٦١، الناشر: دار النهضة العربية، الطبعة السادسة (مطورة ومحدثة)، سنة ٢٠١٥، د/ أحمد عوض بلال، مبادئ قانون العقوبات القسم العام المرجع السابق ص ٣٠٤، د/ أحمد شوقي عمر أبو خطوة، المرجع السابق ص ١٨٣، د/ فوزية عبد الستار، شرح قانون العقوبات القسم العام ص ٢٤٨، الناشر: دار النهضة العربية، سنة ١٩٨٧.

(٢) د/ أحمد عوض بلال، مبادئ قانون العقوبات القسم العام المرجع السابق ص ٣٠٤، د/ أحمد شوقي عمر أبو خطوة، المرجع السابق ص ١٨٤، د/ جاسم خريبط خلف، المرجع السابق ص ١١٥-١١٦.

(٣) د/ أحمد فتحي سرور، المرجع السابق ص ٥٦٦-٥٦٧، د/ فوزية عبد الستار، المرجع السابق ص ٢٥٢-٢٥٣.

(٤) د/ رضا إبراهيم عبد الله البيومي، المرجع السابق ص ٨٥٥، د/ رامي متولي القاضي، المرجع السابق ص ١٨١، د/ أحمد عبد الموجود أبو الحمد زكير، المرجع السابق ص ٢٢٨٠.

الاتجاه الثاني: يرى جانب آخر من الفقه أن الاستخدام غير المشروع لتقنية التزييف العميق من الجرائم ذات النتيجة، وتتمثل هذه النتيجة في اصطناع فيديو أو تسجيل مزيف يبدو حقيقيا ولا يتمكن من كشفه إلا المتخصصون[١].

بناء على ذلك فلا يلزم لتحقق الجريمة وفقا للاتجاه الأول سوى التلاعب بالبيانات الشخصية للمجني عليه، فإذا قام الجاني بهذا التصرف فتعتبر الجريمة قد تحققت، في حين أنه يلزم أن تؤدي معالجة البيانات والتلاعب بها إلى إنتاج فيديو أو تسجيل مزيف يتضمن نسبة أقوال للمجني عليه وهو لم يتقول بها أساسا، أو يظهره في حالة الإتيان ببعض تصرفات لم يأتها، فإذا لم يتم اصطناع الفيديو أو التسجيل وتوقف النشاط في مراحله الأولى، أو تم الاصطناع إلا أنه لا يبدو حقيقا بل مشوها ويمكن كشفه، فلا تعتبر الجريمة متحققة، وإنما تكون قد توقفت في مرحلة الشروع وسيأتي تفصيل ذلك لاحقا.

٣- **علاقة السببية**:

تعد علاقة السببية العنصر الثالث من عناصر الركن المادي للجريمة، ويقصد بها الرابطة التي تصل بين السلوك الإجرامي والنتيجة الإجرامية ، فهي حلقة الاتصال بين النشاط والأثر، بحيث يمكن القول بأن النتيجة ثمرة للنشاط[٢]، غير أن أهمية علاقة السببية تقتصر على جرائم ذات نتيجة مادية، ولا تمتد إلى الجرائم ذات نتيجة قانونية فقط[٣]، ويترتب على عدم تحقق هذا العنصر انتفاء مسئولية الجاني عن جريمة تامة، وإنما يسأل حينئذ عن الشروع في الجريمة،

---

(١) د/ محمود سلامة عبد المنعم الشريف، المرجع السابق ص ٤٢٠-٤٢١.

(٢) د/ محمود نجيب حسني، علاقة السببية في قانون العقوبات ص ٣، دون دار نشر، سنة ١٩٨٣، د/ أحمد فتحي سرور، المرجع السابق ص ٦١٥، د/ أحمد عوض بلال، مبادئ قانون العقوبات القسم العام المرجع السابق ص ٣٠٩، د/ أمين مصطفى محمد، المرجع السابق ص ٢٣٤، د/ إبراهيم عيد نايل، المرجع السابق ص ١٥٠-١٥١.

(٣) د/ أحمد فتحي سرور، المرجع السابق ص ٦١٥، د/ جاسم خريبط خلف، المرجع السابق ص ١١٧.

وذلك إذا كانت الجريمة المرتكبة من الجرائم العمدية، حيث لا شروع في الجرائم غير العمدية[١].

وبالنسبة للاستخدام غير المشروع لتقنية التزييف العميق (Deep fake) فقد سبق أنها من جرائم السلوك المادي وفقا للاتجاه الأول، وبالتالي لا يستلزم تحققها تحقيق نتيجة معينة، فمجرد معالجة البيانات الشخصية والتلاعب بها يحقق الجريمة، واستهدف المشرع من وراء ذلك حماية الحياة الخاصة للأفراد، وبناء على ذلك فإن الاستخدام غير المشروع لتقنية التزييف العميق وفقا لهذا التشريع من الجرائم ذات النتيجة القانونية، فلا يستلزم لتحقيقها علاقة السببية، لأنها تقتصر على جرائم ذات نتيجة مادية.

أما بالنسبة للاتجاه الثاني فيلزم أن يكون بين النتيجة الإجرامية والنشاط الإجرامي علاقة السببية، وذلك بأن يكون الثاني سببا في الأول، فيلزم أن يترتب على معالجة البيانات والتلاعب بها اصطناع فيديو أو تسجيل يبدو حقيقيا لا يتمكن من كشفه الأفراد العاديون، ولكن إذا توقف النشاط ولم يتم اصطناعه، أو تم ولكنه لا يبدو حقيقيا فحينئذ تعتبر الجريمة غير متحققة، وإنما تتوافر حالة الشروع وسيأتي تفصيل ذلك لاحقا.

ثانيا: الركن المعنوي لجريمة التزييف العميق:

سبق بيان أن الركن المادي يتمثل في الإرادة الآثمة، ولكن إرادة الجاني قد تتخذ صورة الخطأ العمدي أو القصد الجنائي، وذلك إذا اتجهت إلى الفعل ونتائجه، وقد تتخذ صورة الخطأ غير العمدي، وذلك إذا اتجهت إلى الفعل دون نتائجه، غير أنه يجب أن يتوقع حدوث النتائج عن الفعل الذي يرتكب، أو على الأقل يمكن أن يتوقع حدوثها[٢].

---

(١) د/ فوزية عبد الستار، المرجع السابق ص ٢٥٥، د/ أحمد شوقي عمر أبو خطوة، المرجع السابق ص ١٨٦.

(٢) د/ فوزية عبد الستار، المرجع السابق ص ٤٧٥، د/ أحمد شوقي عمر أبو خطوة، المرجع السابق ص ٢٢٨.

وتعد جريمة الاستخدام غير المشروع لتقنية التزييف العميق (Deep fake) من الجرائم العمدية، وقد نص على ذلك المشرع المصري في المادة (٢٦) من القانون رقم (١٧٥) لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات، حيث تنص على أنه:" يعاقب..... كل من تعمد استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية ...."، ويفهم ذلك أيضا من عبارات باقي التشريعات، إذ القيام بمعالجة البيانات المتعلقة بالغير عبر استخدام تقنية المعلومات أو مزج أو تركيب الصور والتسجيلات المتعلقة به عبر هذه التقنية يستلزم التعمد وتوجيه الإرادة إلى ذلك، وبالإضافة إلى ذلك فإن طبيعة هذه الجريمة تقتضي ذلك، لأن تنفيذها يستوجب معرفة الجاني التعامل مع تقنية المعلومات والتكنولوجيا الإلكترونية، فهذه الجريمة لا يتصور ارتكابها عن طريق الخطأ غير العمدي.

ولما كانت هذه الجريمة من الجرائم العمدية فإن الركن المعنوي لها يتخذ صورة القصد الجنائي، ويقصد به علم الجاني بكافة العناصر التي استلزمها المشرع لقيام الجريمة واتجاه إرادته إلى تحقيق النتيجة المترتبة عليها[١]، ويقوم هذا القصد على عنصرين هما: العلم والإرادة، فلا يتحقق إلا باجتماعهما، ويترتب على انتفاء أحدهما انتفاء القصد الجنائي، وبالتالي لا يسأل الجاني عن الجريمة العمدية[٢]، وتفصيلهما على النحو التالي:

١- عنصر العلم:

يقصد بالعلم الحالة النفسية التي تقوم في ذهن الجاني، وجوهرها الوعي بحقيقة الأفعال التي يتكون منها الركن المادي للجريمة، مع تمثل أو توقع النتيجة التي يمكن

---

(١) د/ محمد محيي الدين عوض، المرجع السابق ص ٣٤٥، د/ أحمد فتحي سرور، المرجع السابق ص ٦٤٦، د/ أحمد شوقي عمر أبو خطوة، المرجع السابق ص ٢٣٢.

(٢) د/ أحمد عوض بلال، مبادئ قانون العقوبات القسم العام المرجع السابق ص ٦٧٣، د/ فوزية عبد الستار، المرجع السابق ص ٤٧٩، د/ إبراهيم عيد نايل، المرجع السابق ص ٢٠٣-٢٠٤.

أن يحدثها النشاط الإجرامي[١]، والأصل أنه يجب أن ينصرف علم الجاني إلى كافة عناصر الجريمة، فيلزم أن يعلم الجاني النشاط الإجرامي الذي يأتيه، والنتائج المترتبة عليه، وأن يتوقع علاقة السببية التي تربط بين نشاطه والنتيجة، كما يجب أن يعلم الشروط المفترضة أو الأولية إذا استلزمها المشرع، وأن يعلم المصلحة المحمية جنائيا، وأن فعله يشكل خطورة عليه، ويلزم أيضا علمه بتجريم القانون للفعل الذي يأتيه، إلا أن المشرع قد افترض علم الناس بالقانون، وبالتالي لا يعذر بالجهل بالقانون إلا في حالة توافر قوة قاهرة يستحيل معها علم الجاني بالقانون[٢].

وبناء على ذلك يجب أن يعلم الجاني أنه يستخدم تقنية المعلومات لاصطناع فيديو أو تسجيل مزيف خاص بالمجني عليه عبر تقنية التزييف العميق(Deep fake)، والذي يتضمن نسبة قول إليه لم يتقول به، أو نسبة واقعة أو تصرف إليه لم يقم به فعليا على أرض الواقع، وأنه يقوم بربط البيانات التي حصل عليها بمحتوى مناف للآداب العامة وفقا للتشريع المصري والسوري، أو يقوم بمعالجة البيانات بقصد الإضرار بالغير وفقا للتشريع الليبي، فإذا لم يكن الجاني عالما بذلك كأن قام بمعالجة البيانات بغرض حميد كأن يقصد التعليم إلا أنه أخطأ ونتج عن ذلك ربط الفيديو بمحتوى مخالف للآداب العامة فلا يتحقق القصد الجنائي[٣].

---

(١) د/ محمد زكي أبو عامر، قانون العقوبات القسم العام المرجع السابق ص ٢٤٤.

(٢) د/ محمود نجيب حسني، النظرية العامة للقصد الجنائي المرجع السابق ص ٦١ وما بعدها، د/ أحمد شوقي عمر أبو خطوة، المرجع السابق ص ٢٣٦ وما بعدها، د/ جاسم خريبط خلف، المرجع السابق ص ١٢٨ وما بعدها.

(٣) د/ رضا إبراهيم عبد الله البيومي، المرجع السابق ص ٨٥٦، د/ رامي متولي القاضي، المرجع السابق ص ١٨١، د/ أحمد عبد الموجود أبو الحمد زكير، المرجع السابق ص ٢٢٨٤.

٢- عنصر الإرادة:

تعد الإرادة العنصر الثاني للقصد الجنائي، ويقصد بها النشاط النفسي الذي يتجه إلى تحقيق غرض معين عن طريق وسيلة معينة،[١]، وهذا العنصر يستلزم الوعي والإدراك لكونه نشاطا نفسيا، وبالتالي يقتضي العلم بالغرض المراد تحقيقه، والوسيلة التي يستعان بها لتحقيق ذلك الغرض، ويعتبر الغرض هدفا قريبا للإرادة، إذ إن لها هدفا بعيدا أيضا، وهو الغاية، التي تتمثل في إشباع الحاجة[٢].

وعنصر الإرادة في جريمة الاستخدام غير المشروع يتمثل في اتجاه إرادة الجاني إلى الإتيان بالسلوك الإجرامي لهذه الجريمة، وإرادة تحقيق النتيجة التي تتمثل في اصطناع فيديو أو تسجيل مزيف للمجني عليه عبر استخدام تقنية التزييف العميق (Deep fake)[٣]، وربط البيانات التي تمت معالجتها بمحتوى مناف للآداب العامة، أو إظهارها بصورة تمس شرف المجني عليه واعتباره وفقا للتشريع المصري والسوري، أو اتجاه إرادته إلى الإضرار به وفقا للتشريع الليبي، في حين أن المشرع الإماراتي اكتفى بالتلاعب بالبيانات ومعالجتها، وبالتالي لا يستلزم تحقق الجريمة قصد الإضرار أو ربط هذه البيانات بمحتوى مناف للآداب العامة.

ثالثا: الشروع في جريمة التزييف العميق:

يقصد بالشروع : السلوك الذي لم يؤد إلى تحقيق النتيجة التي كان الجاني يسعى إليها بسبب تدخل عامل خارج عن إرادته، فالجاني يأتي بجميع الأعمال اللازمة

---

(١) د/ فوزية عبد الستار، المرجع السابق ص ٤٩١، د/ إبراهيم عيد نايل، المرجع السابق ص ٢١٣، د/ جاسم خريبط خلف، المرجع السابق ص ١٣١.

(٢) د/ محمود نجيب حسني، النظرية العامة للقصد الجنائي المرجع السابق ص ٢٠٢-٢٠٤.

(٣) د/ محمود سلامة عبد المنعم الشريف، المرجع السابق ص ٤٢٩، د/ أشرف سيد أبو العلا، المرجع السابق ص ٥٠٦، د/ محمد على سويلم، المرجع السابق ص ٤٢٢.

لتحقيق النتيجة ومع ذلك لا تتحقق بسبب أمر غير إرادي[١]، وينقسم إلى شروع تام حيث ينفذ الجاني نشاطه الإجرامي كاملا ومع ذلك لا تتحقق النتيجة، ويسمى هذا القسم من الشروع بالجريمة الخائبة، و شروع ناقص حيث يبذل الجاني نشاطه الإرادي لارتكاب الجريمة، ولكنه يتوقف قبل تمامه، وبالتالي لا تتحقق النتيجة، ففي هذا القسم من الشروع لم يتم النشاط نفسه، ويسمى بالجريمة الموقوفة[٢].

وبناء على ما سبق فإن الشروع الناقص يتصور في الاستخدام غير المشروع لتقنية التزييف العميق، بأن يبدأ الجاني بمعالجة البيانات الشخصية المتعلقة بالمجني عليه والتلاعب بها بهدف اصطناع فيديو أو تسجيل مزيف، ولكن نشاطه الإجرامي لم يتم نتيجة سهو في إحدى الخطوات أو نتيجة خطأ تقني ما، أما الشروع التام فلا يتصور إلا بناء على رأي من يعتبر الاستخدام غير المشروع لتقنية التزييف العميق من الجرائم ذات النتيجة المادية، لأن هذا القسم من الشروع يفترض وجود النتيجة في الركن المادي للجريمة، بخلاف جرائم السلوك فلا يفترض ذلك، وإنما تتحقق الجريمة بمجرد ارتكاب الجريمة، فيتحقق الشروع التام وفقا لهذا الرأي في حالة اصطناع فيديو أو تسجيل مزيف إلا أن جودته سيئة، أو كان مشوها في الصورة والصوت، لا تظهر فيه ملامح المجني عليه أو لا يمكن تشخيص صوته، وبالتالي لا تحدد شخصيته[٣].

---

(١) د/ رمسيس بهنام، المرجع السابق ص ٥٨٣، د/ محمد محيي الدين عوض، المرجع السابق ص ٢٠٣، د/ أحمد عوض بلال، مبادئ قانون العقوبات القسم العام المرجع السابق ص ٣٢٤.

(٢) د/ سمير الشناوي، الشروع في الجريمة «دراسة مقارنة» ص ٣ وما بعدها، الناشر: دار النهضة العربية، سنة ١٩٧١، د/ أحمد فتحي سرور، المرجع السابق ص ٥٩٩، د/ إبراهيم عيد نايل، المرجع السابق ص ١٩٣ – ١٩٤، د/ فوزية عبد الستار، المرجع السابق ص ٣٠٤.

(٣) د/ محمود سلامة عبد المنعم الشريف، المرجع السابق ص ٤٢٢.

ولقد عاقب على الشروع في جريمة الاستخدام غير المشروع لتقنية التزييف العميق كل من المشرع الإماراتي في المادة (٥٧) من قانون مكافحة الشائعات والجرائم الإلكترونية، والمشرع المصري في المادة (٤٠) من قانون جرائم تقنية المعلومات، والمشرع السوري في المادة (٣٢) من قانون الجرائم المعلوماتية.

أما المشرع الليبي فلم يُورد في قانون الجرائم الإلكترونية أي نص يدل على معاقبة الشروع، وإن كان قد اعتبر الامتناع عن التبليغ جريمة، سواء علم الممتنع عن الإبلاغ بارتكاب الجريمة أو الشروع فيها، حيث تنص الفقرة الأولى من المادة (٣٥) من القانون سالف الذكر على أنه:" يعاقب بالحبس وبغرامة لا تزيد على ٣,٠٠٠ ثلاثة آلاف دينار كل من علم بارتكاب أي من الجرائم المنصوص عليها في هذا القانون أو بالشروع فيها وكان بإمكانه تبليغ الجهات المختصة ولم يفعل".

المطلب الثالث

العقوبة المقررة لجريمة التزييف العميق (Deep fake)

العقوبة المقررة للاستخدام غير المشروع لتقنية التزييف العميق (Deep fake) قد تكون أصيلة، أو تبعية، أو تكميلية، ويقصد بالأولى: العقوبات التي فرضها المشرع بالشكل الأساس، والتي يتضمن الإيلام الأصيل للجريمة، ولهذا لا يتوقف الحكم فيها على الحكم بعقوبة أخرى، بل يمكن الحكم بها منفردة، ويقصد بالثانية العقوبات التي تتبع العقوبات الأصيلة بقوة القانون، فتطبق ولو لم ينص عليها في الحكم، فمجرد النطق بالعقوبة الأصيلة يتضمن الحكم بالعقوبة التبعية التي نص عليها القانون، سواء ورد في منطوق الحكم أو لا، ويجب أن تنفذها السلطة التنفيذية من تلقاء نفسها، والمقصود بالعقوبة التكميلية تلك التي تتبع العقوبة الأصيلة ويلزم أن ترد في منطوق الحكم[1]، وبالإضافة إلى ذلك قد تتوافر ظروف تقتضي تشديد العقاب، أو تقتضي تخفيفها، أو إعفاء الجاني من العقوبة أصلا، وتفصيل ذلك على النحو التالي:

---

(١) د/ أحمد عوض بلال، النظرية العامة للجزاء الجنائي ص ٢٧٨-٢٨١، الناشر: دار النهضة العربية، الطبعة الثانية، سنة ١٩٩٦، د/ رمسيس بهنام، المرجع السابق ص ٩٠٧، د/ أحمد فتحي سرور، المرجع السابق ص ٩٤٨-٩٤٩، د/ على عبد القادر القهوجي، شرح قانون العقوبات القسم العام (المسئولية الجنائية – أساسها، عوارضها - والجزاء الجنائي- العقوبة، التدابير الاحترازية) ص ١٧٣-١٧٤، الناشر: دار الجامعة الجديدة، ، سنة ٢٠١٠، د/ جاسم خريبط خلف، المرجع السابق ص ٢٨٠، ٢٨٧.

أولا: العقوبات الأصيلة:

١- الحبس:

يعد الحبس[١] عقوبة الاستخدام غير المشروع لتقنية التزييف العميق (Deep fake)، وقد نص على ذلك المشرع الإماراتي في المادة (١٣) من مرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ في شأن مكافحة الشائعات والجرائم الإلكترونية، غير أنه لم يحدد حده الأدنى والأقصى مما يعني أنه لا يجوز أن يقل الحد الأدنى للحبس عن شهر ولا يزيد حده الأقصى على ثلاث سنوات، وذلك وفقا لقانون العقوبات الاتحادي رقم (٣) لسنة ١٩٨٧، ونص عليه المشرع المصري في المادة (٢٦) من القانون رقم (١٧٥) لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات، ولكنه استلزم ألا تقل المدة عن ستين وألا تزيد عن خمس سنوات.

---

(١) عرف المشرع المصري الحبس في المادة (١٨) من قانون العقوبات رقم (٥٨) لسنة ١٩٣٧ بأنه:" وضع المحكوم عليه في أحد السجون المركزية أو العمومية المدة المحكوم بها عليه، لا يجوز أن تنقض هذه المدة عن أربعة وعشرين ساعة، لا تزيد على ثلاث سنين إلا في الأحوال الخصوصية المنصوص عليها قانونا"، عرفه المشرع الإماراتي في المادة (٦٩) من قانون العقوبات رقم (٣) لسنة ١٩٨٧ بأنه:" وضع المحكوم عليه في إحدى المنشآت المخصصة قانونا لهذا الغرض، ذلك للمدة المحكوم بها، لا يجوز أن يقل الحد الأدنى للحبس عن شهر ولا يزيد حده الأقصى على ثلاث سنوات مالم ينص القانون على غير ذلك"، عرفه المشرع الليبي في المادة (٢٢) من قانون العقوبات رقم (٣) لسنة ١٩٥٦ بأنه:" وضع المحكوم عليه في أحد السجون المركزية أو المحلية المدة المحكوم بها عليه، لا يجوز أن تقل هذه المدة بأي حال من الأحوال عن أربع وعشرين ساعة، كما لا يجوز أن تزيد على ثلاث سنوات إلا في الأحوال الخاصة المنصوص عليها قانونا" ولكن لم يتعرض المشرع السوري لتعريف الحبس في قانون العقوبات رقم (٤٨) لسنة ١٩٤٩.

أما المشرع السوري فنص عليه في المادة (٢٦) من القانون رقم ٢٠ لسنة ٢٠٢٢ بشأن الجرائم المعلوماتية، ولكنه استلزم أن تكون المدة المحكوم بها من ستة أشهر إلى سنة، ونص عليه المشرع الليبي في المادة (٢١) من القانون رقم (٥) لسنة ٢٠٢٢ بشأن مكافحة الجرائم الإلكترونية، واستلزم ألا تقل المدة عن السنة، ولكنه لم يحدد الحد الأقصى، غير أنه لا يجوز وفقا للمادة (٢٢) من قانون العقوبات رقم (٣) لسنة ١٩٥٦ أن يتعدى ثلاث سنوات.

٢ـ الغرامة:

تعد الغرامة[١] من العقوبات الأصيلة المقررة لجريمة الاستخدام غير المشروع لتقنية التزييف العميق (Deep fake)، وقد نص عليها المشرع الإماراتي في المادة (١٣) من قانون رقم (٣٤) لسنة ٢٠٢١ بشأن مكافحة الجرائم الإلكترونية والمعلوماتية، ويجب ألا تقل عن خمسين ألف درهم ولا تزيد على خمسمائة ألف درهم، ونص عليها المشرع المصري في المادة (٢٦) من القانون رقم (١٧٥) لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات، واستلزم ألا تقل عن مائة ألف جنيه ولا تجاوز ثلاثمائة ألف جنيه، ونص عليها المشرع السوري في المادة (٢٦) من القانون رقم ٢٠ لسنة ٢٠٢٢ بشأن

---

(١) عرف المشرع المصري الغرامة في المادة (٢٢) من قانون العقوبات رقم (٥٨) لسنة ١٩٣٧ بأنها: " إلزام المحكوم عليه بأن يدفع إلى خزينة الحكومة المبلغ في الحكم، لا يجوز أن تقل الغرامة عن مائة قرش، لا يزيد حدها الأقصى في الجنح على خمسمائة جنيه، ذلك مع عدم الإخلال بالحدود التي يبينها القانون لكل جريمة"، عرفها المشرع الإماراتي في المادة (٧١) من قانون العقوبات رقم (٣) لسنة ١٩٨٧ المستبدلة بمرسوم اتحادي رقم (٧) لسنة ٢٠١٦م بأنها: " إلزام المحكوم عليه أن يدفع للخزينة المبلغ المحكوم به، لا يجوز أن تقل الغرامة عن ألف درهم، لا يزيد حدها الأقصى على مليون درهم في الجنايات، ثلاثمائة ألف درهم في الجنح، ذلك كله ما لم ينص القانون على خلافه"، لكن المشرع السوري لم يتعرض لتعريفها في قانون العقوبات.

الجرائم المعلوماتية، وقدر حدها الأدنى مليون ليرة سورية وحدها الأقصى مليوني ليرة سورية، أما المشرع الليبي فلم يعتبر الغرامة من العقوبات المقررة لجريمة التزييف العميق حيث لم يرد في المادة (٢١) من القانون رقم (٥) لسنة ٢٠٢٢ بشأن مكافحة الجرائم الإلكترونية إلا الحبس فقط.

وجدير بالذكر أنه وفقا للتشريع المصري والإماراتي يملك القاضي سلطة الجمع بين العقوبتين، فيحكم على الجاني بالحبس والغرامة معا، ويملك أيضا سلطة الاختيار بينهما، فيحكم بالحبس وحده أو بالغرامة وحدها، أما المشرع السوري فلم يمنح القاضي هذه السلطة، فلا يجوز أن تقتصر العقوبة على الحبس وحده أو الغرامة وحدها.

ثانيا: العقوبات التكميلية:

١- المصادرة:

تعد مصادرة الأجهزة والبرامج والأدوات والمعدات التي استخدمها الجاني في جريمة التزييف العميق (Deep fake) من العقوبات التكميلية الواجبة الحكم بها[١]، وقد نص على ذلك المشرع الإماراتي في المادة (٥٦) والتي تنص على أنه:" مع عدم الإخلال بحقوق الغير حسن النية، وفي حال الإدانة يحكم بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا

---

(١) لم تعرض التشريعات الأربعة تعريف المصادرة وقد عرفها الفقه بأنها: نزع ملكية المال جبرا بغير مقابل وإضافته إلى ملك الدولة، أو هي تحويل ملكية الأموال ذات الصلة بالجريمة إلى الدولة من غير مقابل. (د/ رمسيس بهنام، المرجع السابق ص ٩٤١، د/ أحمد فتحي سرور، المرجع السابق ص ١٠٠٤، د/ محمد زكي أبو عامر، قانون العقوبات القسم العام المرجع السابق ص ٥٣٧، د/ أحمد عوض بلال، النظرية العامة للجزاء الجنائي المرجع السابق ص ٤٣٥، د/ على عبد القادر القهوجي، المرجع السابق ص ٢٣٥).

المرسوم بقانون أو الأموال المتحصلة منها، وبحذف المعلومات أو البيانات"، ونص عليها المشرع المصري في المادة (٣٨) والتي تنص على أنه:" مع عدم الإخلال بحقوق الغير حسن النية، على المحكمة في حالة الحكم بالإدانة في أي جريمة من الجرائم المنصوص عليها في هذا القانون، أن تقضي بمصادرة الأدوات والآلات والمعدات والأجهزة مما لا يجوز حيازتها قانونا، أو غيرها مما يكون قد استخدم في ارتكاب الجريمة، أو سهل أو أسهم في ارتكابها".

واعتبرها المشرع الليبي من العقوبات التبعية في المادة (٥٠) والتي تنص على أنه:" مع عدم الإخلال بحقوق الغير حسن النية يحكم في جميع الأحوال بمصادرة الأجهزة أو البرامج أو الوسائل المستخدمة في ارتكاب أي من الجرائم المنصوص عليها في هذا القانون أو الأموال المتحصلة منها، كما يحكم بإغلاق المحل أو الموقع الذي ترتكب فيه أي من هذه الجرائم إذا كانت الجريمة قد أُرتكبت بعلم مالكه، إغلاقا كليا أو للمدة التي تقدرها المحكمة".

أما المشرع السوري فاعتبر المصادرة من العقوبات التكميلية الجائزة، فيجوز للقاضي أن يحكم بها أو لا يحكم، حيث تنص المادة (٣٦) من قانون جرائم الإلكترونية رقم (٢٠) لسنة ٢٠٢٢ على أنه:" مع عدم الإخلال بحقوق الغير حسن النية، يجوز للمحكمة مصادرة وسائل تقنية المعلومات أو أي وسائل أخرى تم استعمالها في ارتكاب أي من الجرائم المنصوص عليها في هذا القانون".

وجدير بالذكر أن المشرع المصري والإماراتي اشترطا صدور الحكم بالإدانة، في حين أن المشرع الليبي لم يشترط ذلك، وإنما نص على وجوب المصادرة في جميع الأحوال، سواء صدر الحكم بإدانة المتهم، أو ببراءته.

٢- العزل:

يعد العزل من العقوبات التكميلية وفقا للتشريع المصري، وذلك إذا كان مرتكب الجريمة من الموظفين العمومين ووقعت الجريمة أثناء تأدية الوظيفة أو بسببها، حيث تنص المادة (٣٩) من قانون جرائم تقنية المعلومات رقم (١٧٥) لسنة ٢٠١٨ على أنه:" للمحكمة إذا قضت بالإدانة على أحد الموظفين العموميين، لارتكابه جريمة من الجرائم المنصوص عليها في هذا القانون، أثناء وبسبب تأديته لوظيفته، أن تقضى بعزله مؤقتا من وظيفته، إلا في الحالات المشار إليها في المادة (٣٤) من هذا القانون فيكون العزل وجوبيا".

ثالثا: الظروف المشددة:

١- استخدام تقنية التزييف العميق (Deep fake) في نشر البيانات والأخبار والتقارير المزيفة والكاذبة:

نص على هذا الظرف المشرع الإماراتي في الفقرة الأولى من المادة (٥٢) من قانون مكافحة الشائعات والجرائم الإلكترونية رقم (٣٤) لسنة ٢٠٢١، والتي تنص على أنه:"١- يعاقب بالحبس مدة لا تقل عن سنة والغرامة التي لا تقل عن (١٠٠,٠٠٠) مائة ألف درهم ، كل من استخدم الشبكة المعلوماتية أو وسيلة من وسائل تقنية المعلومات لإذاعة أو نشر أو إعادة نشر أو تداول أو إعادة تداول أخبار أو بيانات زائفة أو تقارير أو إشاعات كاذبة أو مغرضة أو مضللة أو مغلوطة أو تخالف ما تم الإعلان عنه رسمياً، أو بث أي دعايات مثيرة من شأنها تأليب الرأي العام أو إثارته أو تكدير الأمن العام أو إلقاء الرعب بين الناس أو إلحاق الضرر بالمصلحة العامة أو بالاقتصاد الوطني أو بالنظام العام أو بالصحة العامة".

كما أن المشرع الليبي وفقا للفقرة الثانية من المادة (٢١) من قانون مكافحة الجرائم الإلكترونية رقم (٥) لسنة ٢٠٢٢ اعتبر المزج أو التركيب مع صور أو أصوات إباحية

ونشرها عبر شبكة المعلومات الدولية من الظروف المشددة، حيث تنص هذه الفقرة على أنه:" فإذا كان المزج أو التركيب مع صور أو أصوات إباحية ونشرها عبر شبكة المعلومات الدولية أو بأي وسيلة إلكترونية أخرى تكون العقوبة السجن مدة لا تقل عن خمس سنوات".

كذلك اعتبر المشرع السوري نشر البيانات التي تم معالجتها ظرفا مشدد، إذ تنص الفقرة الثانية من المادة (٢٦) من قانون الجرائم المعلوماتية رقم (٢٠) لسنة ٢٠٢٢ على أنه:" وتشدد العقوبة لتصبح الحبس من سنة إلى سنتين وغرامة من (٢,٠٠٠,٠٠٠) ل.س مليوني ليرة سورية إلى (٣,٠٠٠,٠٠٠) ل.س ثلاثة ملايين ليرة سورية إذا قام الفاعل بنشرها على الشبكة".

٢ـ استخدام تقنية التزييف العميق (Deep fake) في إثارة الرأي العام:

اعتبر المشرع الإماراتي نشر الأخبار والتقارير المزيفة لإثارة الرأي العام من الظروف المشددة، حيث تنص الفقرة الثانية من المادة (٥٢) على أنه:" وتكون العقوبة الحبس مدة لا تقل عن (٢) سنتين والغرامة التي لا تقل عن (٢٠٠,٠٠٠) مائتي ألف درهم إذا ترتب على أي من الأفعال المذكورة بالبند (١) من هذه المادة تأليب الرأي العام أو إثارته ضد إحدى سلطات الدولة أو مؤسساتها أو إذا ارتكبت بزمن الأوبئة والأزمات والطوارئ أو الكوارث".

٣ـ استخدام تقنية التزييف العميق (Deep fake) للإخلال بالمصالح السيادية والاقتصادية للدولة:

نص المشرع الإماراتي في الفقرة الثالثة من المادة (٦٠) من قانون مكافحة الشائعات والجرائم الإلكترونية رقم (٣٤) لسنة ٢٠٢١ على اعتبار ارتكاب أي جريمة من الجرائم المنصوص عليها في هذا القانون والتي من ضمنها التزييف العميق (Deep fake) لحساب أو مصلحة دولة أجنبية أو لجماعة معادية أو إرهابية أو أي

تنظيم غير مشروع، حيث تنص هذه الفقرة على أنه:" في تطبيق أحكام هذه المرسوم بقانون يعد ظرفا مشددا: ٣- ارتكاب الجاني أي جريمة منصوص عليها في هذا المرسوم بقانون لحساب أو لمصلحة دولة أجنبية أو أي جماعة معادية أو جماعة إرهابية أو تنظيم غير مشروع".

وكذلك اعتبر المشرع ارتكاب الجرائم الواردة في قانون مكافحة جرائم تقنية المعلومات رقم (١٧٥) لسنة ٢٠١٨ والتي من ضمنها الاستخدام غير المشروع لتقنية التزييف العميق (Deep fake) ظرفا مشددا إذا كان الغرض منه الإخلال بالمصالح السيادية والاقتصادية للدولة، حيث تنص المادة (٣٤) من القانون سالف الذكر على أنه:" إذا وقعت أي جريمة من الجرائم المنصوص عليها في هذا القانون بغرض الإخلال بالنظام العام أو تعريض سلامة المجتمع وأمنه للخطر، أو الإضرار بالأمن القومي للبلاد أو بمركزها الاقتصادي أو منع أو عرقلة ممارسة السلطات العامة لأعمالها، أو تعطيل أحكام الدستور أو القوانين أو اللوائح أو الإضرار بالوحدة الوطنية والسلام الاجتماعي تكون العقوبة السجن المشدد".

٤- الاستخدام غير المشروع لتقنية التزييف العميق (Deep fake) بمناسبة أو بسبب تأدية العمل:

اعتبر المشرع الإماراتي ارتكاب جريمة من الجرائم الواردة في قانون مكافحة الشائعات والجرائم الإلكترونية بمناسبة أو بسبب أداء العمل ظرفا مشددا، حيث تنص الفقرة الأولى من المادة (٦٠) من القانون سالف الذكر على أنه:" في تطبيق أحكام هذا المرسوم بقانون يعد ظرفا مشددا: ١ - ارتكاب الجاني لأي جريمة منصوص عليها في هذا المرسوم بقانون بمناسبة أو بسبب تأدية عمله".

ونص المشرع السوري أيضا على اعتبار استغلال الجاني وظيفته لارتكاب الجرائم الواردة في قانون الجرائم المعلوماتية رقم ٢٠ لسنة ٢٠٢٢ من الظروف المشددة،

حيث تنص الفقرة الأولى من المادة (٣٣) من القانون آنف الذكر على أنه:" تشدد العقوبة وفق أحكام المادة (٢٤٧) من قانون العقوبات[1] في الحالات التالية: أ- إذا استغل الفاعل وظيفته أو عمله لارتكاب أي من الجرائم المنصوص عليها في هذا القانون".

٥- كون المجني عليه قاصرا:

نص المشرع السوري على تشديد العقوبة إذا كان المجني عليه في الجرائم الواردة في قانون الجرائم المعلوماتية رقم (٢٠) لسنة ٢٠٢٢ والتي من ضمنها الاستخدام غير المشروع لتقنية التزييف العميق (Deep fake) قاصرا، حيث تنص الفقرة الثانية من المادة (٣٣) من القانون آنف الذكر على أنه:" تشدد العقوبة وفق أحكام المادة (٢٤٧) من قانون العقوبات في الحالات التالية: ب- إذا كان المجني عليه في الجرائم المنصوص عليها في هذا القانون قاصراً".

رابعا: الظروف المخففة وحالات الإعفاء:

اعتبر المشرع الإماراتي إخبار الجهات القضائية أو الإدارية بأي معلومة تتعلق بالجرائم الواردة في قانون مكافحة الشائعات والجرائم الإلكترونية والتي من ضمنها الاستخدام غير المشروع لتقنية التزييف العميق (Deep fake) من الظروف المخففة أو الإعفاء من العقاب، شريطة أن يؤدي ذلك إلى كشف الجريمة أو مرتكبيها أو القبض عليهم أو إثباتها عليهم، حيث تنص المادة (٦١) من القانون سالف الذكر على أنه:" ١- تقضي المحكمة، بناء على طلب من النائب العام، بتخفيف العقوبة أو

---

(١) تنص المادة (٢٤٧) من قانون العقوبات السوري رقم (١٤٨) لسنة ١٩٤٩ على أنه:" إذا لم يعين القانون مفعول سبب مشدد، أوجب السبب المذكور تشديد العقوبة على الوجه التالي: يبدل الإعدام من الأشغال الشاقة المؤبدة، تزداد كل عقوبة مؤقتة من الثلث إلى النصف وتضاعف الغرامة.

بالإعفاء منها، عمن أدلى من الجناة إلى السلطات القضائية أو الإدارية بمعلومات تتعلق بأي جريمة من الجرائم المنصوص عليها في هذا المرسوم بقانون، متى أدى ذلك إلى الكشف عن الجريمة ومرتكبيها أو إثباتها عليهم أو القبض على أحدهم. ٢- وفي الجرائم الماسة بأمن الدولة للنائب العام للاتحاد دون غيره أن يطلب من المحكمة المنظورة أمامها الدعوى إعمال حكم الفقرة السابقة في غير الحالات المنصوص عليها فيها، إذا تعلق الطلب بالمصلحة العليا للدولة أو بأي مصلحة وطنية أخرى، فإذا صدر حكم في الدعوى جاز له أن يقدم الطلب إلى المحكمة التي أصدرته قبل التنفيذ أو أثناء التنفيذ".

ونص على مثل ذلك المشرع المصري في المادة (٤١) من قانون جرائم تقنية المعلومات، والتي تنص على أنه:" يعفى من العقوبات المقررة للجرائم المنصوص عليها في هذا القانون، كل من بادر من الجناة أو الشركاء إلى إبلاغ السلطات القضائية أو السلطات العامة بما يعلمه عنها قبل البدء فى تنفيذ الجريمة وقبل كشفها. ويجوز للمحكمة الإعفاء من العقوبة أو التخفيف منها إذا حصل البلاغ بعد كشف الجريمة وقبل التصرف في التحقيق فيها، إذا مكن الجاني أو الشريك في أثناء التحقيق السلطات المختصة من القبض على مرتكبي الجريمة الآخرين، أو على ضبط الأموال موضوع الجريمة، أو أعان أثناء البحث والتحقيق على كشف الحقيقة فيها، أو على القبض على مرتكبي جريمة أخرى مماثله لهذا النوع والخطورة. ولا يخل حكم هذه المادة، بوجوب الحكم برد المال المتحصل من الجرائم المنصوص عليها بالقانون".

خامسا: العقوبة المقررة للشروع في الاستخدام غير المشروع لتقنية التزييف العميق:

لقد عاقب المشرع المصري والإماراتي والسوري على الشروع في الجرائم الواردة في قوانين الجرائم الإلكترونية وتقنية المعلومات حيث تنص المادة (٥٧) من التشريع الإماراتي على أنه:" يعاقب على الشروع في الجنح المنصوص عليها في هذا المرسوم بقانون بنصف العقوبة المقررة للجريمة التامة" وتنص المادة (٤٠) من التشريع المصري على أنه:" يعاقب كل من شرع فى ارتكاب الجنح المنصوص عليها في هذا القانون، بما لا يجاوز نصف الحد الأقصى للعقوبة المقررة للجريمة"، وتنص المادة (٣٢) من التشريع السوري على أنه:" يعاقب على الشروع في الجنح المنصوص عليها في هذا القانون وفق الأحكام الواردة في قانون العقوبات"[(١)].

(١) تنص الفقرة الثانية من المادة (٢٠١) من قانون العقوبات السوري رقم (١٤٨) لسنة ١٩٤٩ على أنه:" العقوبة المفروضة للجنحة التامة يمكن تخفيضها إلى النصف في الجنحة المشروع فيها، حتى الثلث في الجنحة الناقصة".

الخاتمة:

تتضمن الخاتمة نتائج البحث وتوصياته، وذلك كما يلي:

أولا: نتائج البحث:

١- ترجع نشأة تقنية التزييف العميق إلى سنة ٢٠١٧ حينما قام بعض الأفراد باصطناع فيديو إباحي لإحدى نجمات هوليود، ويمكن استخدام هذه التقنية في إنشاء المحتوى المرئي والصوتي، كما أن حجم استعمالها في ازدياد مستمر.

٢- يتميز التزييف العميق بأنه تقنية تعتمد على الذكاء الاصطناعي والتعلم العميق، ويستهدف مستخدمها معالجة البيانات الشخصية لأحد الأفراد بهدف إنتاج فيديو مزيف يبدو حقيقياً ويتضمن ظهور هذا الشخص في حالة القيام بتصرف من التصرفات التي لم يقم به في الواقع وحقيقة الأمر.

٣- التزييف العميق من السلوكيات العابرة للحدود، فلا يتوقف عند حدود دولة معينة، بل قد يكون المستخدم في دولة والشخص الذي قام المستخدم بتزييف صوره ومحادثاته في دولة أخرى، كما أنه من السلوكيات التي يسهل الإتيان بها لتوافر وسائلها، غير أنه يتسم في الوقت ذاته بصعوبة الكشف، حيث لا يترك أثرا مادياً يمكن الاستفادة منه.

٤- تشتمل تقنية التزييف العميق على مخاطر عديدة، منها المخاطر السياسية المتمثلة في التأثير على الانتخابات والتلاعب بنتائجها، واختلاق الأزمات السياسية، ومنها المخاطر الأمنية المتمثلة في إحداث فجوة بين السلطة التنفيذية والشعب، وإحداث أعمال الشغب ووقوع المظاهرات وزعزعة الأمن في المجتمع.

٥- من المخاطر الاقتصادية لتقنية التزييف العميق الاحتيال والتأثير على البورصة والابتزاز المالي، هذا بالإضافة إلى المخاطر الاجتماعية المتمثلة في التشهير والانتقام

الإباحي والتشكيك في المصداقية ونشر أخبار كاذبة والعبث بأدلة الإثبات والابتزاز الجنسي.

٦- يمثل النشاط الإجرامي للاستخدام غير المشروع لتقنية التزييف العميق في معالجة البيانات الشخصية للأفراد والتلاعب بها عبر استخدام تقنية المعلومات أو شبكة الإنترنت بهدف ربطها بمحتوى مناف للآداب العامة في التشريع المصري والسوري، أو بهدف الإضرار بالغير وفقا للتشريع الليبي.

٧- اختلف الفقه في الاستخدام غير المشروع للتزييف العميق فاعتبره البعض من جرائم السلوك المادي، فيقع بمجرد معالجة البيانات، في حين أن جانباً آخر من الفقه اعتبره من الجرائم ذات النتيجة التي تتمثل في إنتاج فيديو مزيف، فوفقا لهذا الرأي يجب أن تتوافر علاقة السببية بين النشاط والنتيجة.

٨- يعتبر الحبس من العقوبات الأصيلة المقررة للاستخدام غير المشروع لتقنية التزييف العميق في التشريعات الأربعة، بخلاف الغرامة فلا تعتبر كذلك إلا في التشريع المصري والإماراتي والسوري دون التشريع الليبي، غير أن القاضي يملك الحكم بإحدى العقوبتين في التشريعين المصري والإماراتي، بخلاف التشريع السوري فلا يملك ذلك، وبالتالي يجب أن يحكم بهما معا.

٩- تعد مصادرة الأجهزة والبرامج والأدوات والمعدات التي استخدمها الجاني في جريمة التزييف العميق من العقوبات التكميلية في جميع التشريعات، غير أنها وجوبية في كل من التشريع المصري والإماراتي والليبي، أما التشريع السوري فاعتبرها من العقوبات الجوازية، هذا من جهة، ومن جهة أخرى استلزم المشرع المصري والإماراتي صدور الحكم بالإدانة بخلاف المشرع الليبي فلم يشترط ذلك، فيجوز للقاضي أن يحكم بالمصادرة وفقا لهذا التشريع وإن ثبتت براءة المتهم.

١٠ - اعتبر المشرع المصري العزل من العقوبات التكميلية إذا كان مرتكب الجريمة من الموظفين العمومين ووقعت الجريمة أثناء تأدية الوظيفة أو بسببها، في حين أن المشرع الإماراتي والسوري اعتبر ارتكاب الجريمة بمناسبة أو بسبب أداء العمل ظرفا مشددا، أما بالنسبة للتشريع الليبي فلم يرد أي نص في هذا الصدد.

١١ - نص المشرع الإماراتي على اعتبار نشر الأخبار الكاذبة والمزيفة أو إعادة نشرها بهدف إثارة الرأي العام من الظروف المشددة، كما أن المشرع الليبي اعتبر نشر المحتوى الإباحي المزيف من الظروف المشددة أيضا.

١٢ - يعتبر استخدام تقنية التزييف العميق بهدف الإخلال بالمصالح السيادية والاقتصادية من الظروف المشددة وفقا للتشريع المصري والإماراتي، ولم يرد في التشريع السوري والليبي ما يقابل ذلك.

١٣ - اعتبر المشرع السوري بخلاف باقي المشرعين كون المجني عليه قاصرا من الظروف المشددة.

ثانيا: التوصيات والاقتراحات:

١ - تستلزم المواجهة الجنائية لتقنية التزييف العميق التدخل التشريعي وتنظيمها تنظيما واضحا، سواء تم ذلك عن طريق تشريع خاص وهو الأفضل، أو تعديل النصوص الموجودة بما يلائم التقدم التكنولوجي، وذلك لأن النصوص القائمة إما أن تجعل العقوبة المتمثلة في الحبس والغرامة تخييرية كما في التشريع المصري والإماراتي والليبي، أو تستلزم لتحقق الجريمة أن تتم معالجة البيانات بهدف ربطها بمحتوى مناف للآداب العامة كما في التشريع المصري والسوري، أو تشترط أن يتم ذلك بقصد الإضرار بالغير كما في التشريع الليبي، في حين يكفي لوقوع الجريمة مجرد معالجة البيانات والتلاعب بها.

٢- تشديد العقوبة المقررة للاستخدام غير المشروع لتقنية التزييف العميق بشكل عام، وذلك لانتشاره يوما بعد يوم، لا سيما إذا استخدمها الجاني في التجسس للدول الأجنبية أو المنظمات الإرهابية أو نتج عن ذلك الإضرار بمصالح الدولة السياسية والاقتصادية والعسكرية.

٣- يلزم تشديد العقوبة أيضا إذا كان الهدف من استخدام تقنية التزييف العميق إنتاج فيديو إباحي مزيف أو يمس شرف المجني عليه واعتباره، أو كان الضحية امرأة أو طفلا، أو أدى إلى الانتحار.

٤- يجب تشديد العقوبة إذا كان الجاني من الموظفين واستخدم تقنية التزييف العميق بناء على سلطته الوظيفية، سواء كان من الموظفين العمومين، أو من أصحاب المهن الحرة نحو المحامين أو أصحاب استديوهات التصوير، أو كان الجاني من أقرباء المجني عليه وأصحابه أو ممن له السلطة عليه.

٥- عدم مؤاخذة الجاني إذا استخدم تقنية التزييف العميق في تحقيق الأهداف المشروعة نحو: الترفيه أو صناعة الأفلام أو نشرة إخبارية أو لأهداف تعليمية وطبية أو خدمة العملاء، أو استخدمها الجاني في إنتاج فيديوهات وتسجيلات مزيفة متعلقة بأحد الأشخاص ولكن برضاه شريطة ألا تتضمن محتوى منافيا للآداب العامة والحياء العام.

٦- إبرام معاهدات دولية تجرم الاستخدام غير المشروع لتقنية التزييف العميق، وتبين كيفية ملاحقة الجاني وتسليم المجرمين، وذلك لأن الاستخدام غير المشروع لتقنية التزييف العميق من الجرائم العابرة للحدود، فمواجهتها يستلزم اتحاد موقف الدول بتجريمها وملاحقة الجاني، كما أن عدم إفلاته من العقاب تستلزم عقد اتفاقات دولية تعالج وتنظم كيفية تسليم المجرمين أيضا.

٧- عقد ندوات يُبحث فيها عن هذه الجريمة وكيفية مواجهتها، وتوعية الناس وحثهم على إبلاغ السلطات المختصة عند وقوعها حتى لا يفلت الجاني عن العقاب بسبب عدم الإبلاغ.

قائمة المراجع:

أولا: الكتب:

١- د/ إبراهيم عيد نايل، قانون العقوبات القسم العام «النظرية العامة للجريمة»، الناشر: دار النهضة العربية، سنة ٢٠٢٠.

٢- د/ أحمد شوقي عمر أبو خطوة، شرح الأحكام العام لقانون العقوبات، الناشر: دار النهضة العربية، دون تاريخ النشر.

٣- د/ أحمد عوض بلال، النظرية العامة للجزاء الجنائي، الناشر: دار النهضة العربية، الطبعة الثانية، سنة ١٩٩٦.

٤- د/ أحمد عوض بلال، مبادئ قانون العقوبات المصري القسم العام، الناشر: دار النهضة العربية، سنة ٢٠١٠.

٥- د/ أحمد فتحي سرور، الوسيط في قانون العقوبات القسم العام، الناشر: دار النهضة العربية، الطبعة السادسة «مطورة ومحدثة»، سنة ٢٠١٥.

٦- د/ أمين مصطفى محمد، قانون العقوبات القسم العام (النظرية العامة للجريمة)، الناشر: منشورات الحلبي الحقوقية، الطبعة الأولى، سنة ٢٠١٠.

٧- د/ جاسم خريبط خلف، شرح قانون العقوبات القسم العام، الناشر: منشورات زين الحقوقية بيروت -لبنان، الطبعة الثالثة، دون تاريخ النشر.

٨- د/ رامي متولي القاضي، شرح قانون مكافحة جرائم تقنية المعلومات رقم (١٧٥) لسنة ٢٠١٨ مقارنا بالتشريعات المقارنة والمواثيق الدولية، الناشر: مركز الدراسات العربية، الطبعة الأولى ١٤٤١هـ -٢٠٢٠.

٩- د/ رمسيس بهنام، النظرية العامة للقانون الجنائي، الناشر: منشأة المعارف بالإسكندرية، الطبعة الأولى سنة ١٩٩٩.

١٠ – د/ على عبد القادر القهوجي، شرح قانون العقوبات القسم العام (المسئولية الجنائية – أساسها، عوارضها –والجزاء الجنائي–العقوبة، التدابير الاحترازية)، الناشر: دار الجامعة الجديدة، سنة ٢٠١٠.

١١ – د/ محمد زكي أبو عامر، قانون العقوبات القسم العام، الناشر: منشأة المعارف بالإسكندرية، سنة ١٩٩٣.

١٢ – د/ محمد زكي أبو عامر، الحماية الجنائية للعرض في التشريع المصري، الناشر: الفنية للطباعة والنشر، سنة ١٩٨٥.

١٣ – د/ محمد على سويلم، شرح قانون جرائم تقنية المعلومات، الناشر: دار المطبوعات الجامعية، الطبعة الأولى ٢٠١٩.

١٤ – د/ محمد محيي الدين عوض، القانون الجنائي مبادئه الأساسية ونظرياته العامة «دراسة مقارنة»، الناشر: مطبعة جامعة القاهرة والكتاب الجامعي، سنة ١٩٨١.

١٥ – د/ محمد ناجي ياقوت، فكرة الحق في السمعة ، الناشر: منشأة المعارف بالإسكندرية جلال حزي و شركاه، دون عدد الطبع وتاريخ النشر.

١٦ – د/ محمود نجيب حسني، النظرية العامة للقصد الجنائي دراسة تأصيلية مقارنة للركن المعنوي في الجرائم العمدية، الناشر: دار النهضة العربية، سنة ٢٠٠٦.

١٧ – د/ محمود نجيب حسني، شرح قانون العقوبات القسم الخاص، الناشر: دار المطبوعات الجامعية، الطبعة السادسة، سنة ٢٠١٩م.

١٨ – د/ محمود نجيب حسني، علاقة السببية في قانون العقوبات، دون دار نشر، سنة ١٩٨٣.

١٩ – د/ ة فوزية عبد الستار، شرح قانون العقوبات القسم العام، الناشر: دار النهضة العربية، سنة ١٩٨٧.

٢٠ـ د/ سمير الشناوي، الشروع في الجريمة دراسة مقارنة، الناشر: دار النهضة العربية، سنة ١٩٧١،

ثانيا: الرسائل العلمية:

٢١- د/ عبد الرحمن محمد إبراهيم خلف، الحماية الجنائية للحق في الشرف دراسة تحليلية تأصيلية، رسالة دكتوراه، كلية الحقوق جامعة القاهرة ١٩٩٢م.

ثالثا: البحوث:

٢٢- د/ أحمد عبد الموجود أبو الحمد زكير، جريمة التزييف الإباحي العميق دراسة مقارنة، بحث منشور بمجلة القانونية، جامعة القاهرة، كلية الحقوق، فرع الخرطوم، المجلد ١١، العدد ٧، سنة ٢٠٢٢.

٢٣- د/ أحمد محمد فتحي الخولي، المسئولية المدنية الناتجة عن الاستخدام غير المشروع لتطبيقات الذكاء الاصطناعي «الديب فيك نموذجا»، بحث منشور في مجلة البحوث الفقهية والقانونية، جامعة الأزهر، كلية الشريعة والقانون بدمنهور، المجلد ٣٣، العدد ٣٦، أكتوبر ٢٠٢١م.

٢٤- د/ أحمد مصطفى معوض محمد محرّم، استخدامات الذكاء الاصطناعي (AI)، استخدام تقنية التزييف العميق (Deep fake) في قذف الغير نموذجا «دراسة فقهية مقارنة معاصرة»، بحث منشور في مجلة البحوث الفقهية والقانونية، العدد التاسع والثلاثون، إصدار أكتوبر ١٤٤٤هـ – ٢٠٢٢م.

٢٥- د/ أشرف سيد أبو العلا، المواجهة الجنائية لتقنية الديب فيك Deep fakes، بحث منشور في مجلة العلوم القانونية والاقتصادية، جامعة عين شمس، كلية الحقوق، المجلد ٦٦، العدد ٣، يناير ٢٠٢٤.

٢٦- د/ رضا إبراهيم عبد الله البيومي، الحماية القانونية من مخاطر تطبيقات التزييف العميق في الفقه الإسلامي والقانون الوضعي دراسة تحليلية مقارنة، بحث منشور في مجلة روح القوانين، جامعة طنطا، كلية الحقوق، عدد خاص- المؤتمر الدولي الثامن- التكنولوجيا والقانون.

٢٧- د/ محمود سلامة عبد المنعم الشريف، جريمة الانتقام الإباحي عبر تقنية التزييف العميق (Deep fakes) والمسؤولية الجنائية عنها، بحث منشور في مجلة الحقوق للبحوث القانونية والاقتصادية، جامعة الإسكندرية، كلية الحقوق، العدد الأول، يوليو ٢٠٢٢.

٢٨- د/ ولاء محمد محروس الناغي، ود/ ياسر محمد محروس الناغي، إدراك مستخدمي مواقع التواصل الاجتماعي لتهديدات التزييف العميق (Deep fakes) وعلاقته بالاستخدام الآمن لتلك المواقع، بحث منشور في مجلة العلمية لبحوث الصحافة، جامعة القاهرة، كلية الإعلام، العدد الرابع والعشرون الجزء الثالث، يوليو/ ديسمبر ٢٠٢٢م.

رابعا: التقارير:

٢٩- دليل التزييف العميق الصادر عن البرنامج الوطني للذكاء الاصطناعي، الإمارات العربية المتحدة، يوليو سنة ٢٠٢١م.

٣٠- الذكاء الاصطناعي و مخاطر التزييف العميق، تقرير دوري يصدر عن مركز المعلومات ودعم اتخاذ القرار التابع لمجلس الوزراء المصري، نشر بتاريخ ٢٥ مارس ٢٠٢٣.

References:

1: alkutub:

• d/ 'iibrahim eid nayil, qanun aleuqubat alqism aleamu <<alnazariat aleamat liljarimati>>, alnaashir: dar alnahdat alearabiati, sanat 2020.

• d/ 'ahmad shawqi eumar 'abu khutwat, sharah al'ahkam aleami liqanun aleuqubati, alnaashir: dar alnahdat alearabiat, dun tarikh alnashri.

• d/ 'ahmad eawad bilali, alnazariat aleamat liljaza' aljanayiy, alnaashir: dar alnahdat alearabiati, altabeat althaaniatu, sanat 1996.

• d/ 'ahmad eawad bilal, mabadi qanun aleuqubat almisrii alqism aleama, alnaashir: dar alnahdat alearabiati, sanat 2010.

• d/ 'ahmad fathi srur, alwasit fi qanun aleuqubat alqism aleama, alnaashir: dar alnahdat alearabiati, altabeat alsaadisa <<mtawirat wamuhdithatun>>, sanat 2015.

• d/ 'amin mustafaa muhamad, qanun aleuqubat alqism aleamu (alnazariat aleamat liljarimati), alnaashir: manshurat alhalabi alhuquqiati, altabeat al'uwlaa, sanat 2010.

• d/ jasim khiribit khalfa, sharah qanun aleuqubat alqism aleama, alnaashir: manshurat zayn alhuquqiat bayrut -lubnan, altabeat althaalithata, dun tarikh alnashri.

• da/ rami mutualiy alqadi, sharh qanun mukafahat jarayim taqniat almaelumat raqm (175) lisanat 2018 muqaranan bialtashrieat almuqarinat walmawathiq alduwaliata, alnaashir: markaz aldirasat alearabiati, altabeat al'uwlaa 1441hi -2020.

• da/ ramsis bihnami, alnazariat aleamat lilqanun aljanayiyi, alnaashir: munsha'at almaearif bial'iiskandariati, altabeat al'uwlaa sanat 1999.

• da/ ealaa eabd alqadir alqahwaji, sharh qanun aleuqubat alqism aleamu (almasyuwliat aljinayiyat - 'asasiha, eawariduha -waljaza' aljinayiy-aleuqubati, altadabir alaihtiraziatu), alnaashir: dar aljamieat aljadidati, sanat 2010.

• d/ muhamad zaki 'abu eamir, qanun aleuqubat alqism aleama, alnaashir: munsha'at almaearif bial'iiskandariati, sanat 1993.

• d/ muhamad zaki 'abu eamir, alhimayat aljinayiyat lileard fi altashrie almisrii, alnaashiru: alfaniyat liltibaeat walnashri, sanat 1985.

• d/ muhamad ealaa suilami, sharh qanun jarayim tiqniat almaelumati, alnaashir: dar almatbueat aljamieiati, altabeat al'uwlaa 2019.
• d/ muhamad muhyi aldiyn eawad, alqanun aljinayiyu mabadiah al'asasiat wanazariaatih aleama <<dirasat muqaranati>>, alnaashir: matbaeat jamieat alqahirat walkutaab aljamieii, sanat 1981.
• d/ muhamad naji yaqut, fikrat alhaqi fi alsumeat , alnaashir: munsha'at almaearif bial'iiskandariat jalal hizi washarakah, dun eadad altabe watarikh alnashri.
• d/ mahmud najib hasni, alnazariat aleamat lilqasd aljinayiyi dirasat tasiliat muqaranatan lilrukn almaenawii fi aljarayim aleamdiati, alnaashir: dar alnahdat alearabiati, sanat 2006.
• d/ mahmud najib hasni, sharah qanun aleuqubat alqism alkhasa, alnaashir: dar almatbueat aljamieiati, altabeat alsaadisati, sanatan 2019m.
• d/ mahmud najib hasni, ealaqat alsababiat fi qanun aleuqubati, dun dar nashra, sanat 1983.
• di/t fawziat eabd alsatar, sharh qanun aleuqubat alqism aleama, alnaashir: dar alnahdat alearabiati, sanat 1987.
• du/ samir alshanawi, alshurue fi aljarimat dirasat muqaranati, alnaashir: dar alnahdat alearabiati, sanat 1971,

2: alrasayil aleilmia:

• da/ eabd alrahman muhamad 'iibrahim khalafa, alhimayat aljinayiyat lilhaqi fi alsharaf dirasat tahliliat tasiliata, risalat dukturah, kuliyat alhuquq jamieat alqahirat 1992m.

3: albuhuth:

• d/ 'ahmad eabd almawjud 'abu alhamd zakir, jarimat altazyif al'iibahiu aleamiq dirasat muqaranati, bahath manshur bimajalat alqanuniati, jamieat alqahirat, kuliyat alhuquqi, fare alkhartum, almujalad 11, aleadad 7, sanat 2022.
• d/ 'ahmad muhamad fathi alkhuli, almasyuwliat almadaniat alnaatijat ean alaistikhdam ghayr almashrue litatbiqat aldhaka' alaistinaeii <<aldyb fik namudhaja>>, bahath manshur fi majalat albuhuth alfiqhiat walqanuniati, jamieat al'azhar, kuliyat alsharieat walqanun bidiminhur, almujalad 33, aleadad 36, 'uktubar 2021m.
• du/ 'ahmad mustafaa mueawad muhamad mhrrm, aistikhdamat aldhaka' aliastinaeii (AI), astikhdam tiqniat altazyif aleamiq (Deep fake) fi qadhf alghayr namudhajan <<dirasat fiqhiat muqaranat

mueasirati>>, bahth manshur fi majalat albuhuth alfiqhiat walqanuniati, aleadad altaasie walthalathuna, 'iisdar 'uktubar 1444h - 2022m.

• d/ 'ashraf sayid 'abu alealaa, almuajahat aljinayiyat litiqniat aldiyb fik (Deep fakes bijathi manshur fi majalat aleulum alqanuniat walaiqtisadiati, jamieat eayn shams, kuliyat alhuquqi, almujalad 66, aleadad 3, yanayir 2024.

• d/ rida 'iibrahim eabd allah albaywmi, alhimayat alqanuniat min makhatir tatbiqat altazyif aleamiq fi alfiqh al'iislamii walqanun alwadeiu dirasatan tahliliatan muqaranata, bahath manshur fi majalat ruh alqawanini, jamieat tanta, kuliyat alhuquqi, eadad khasa- almutamar alduwalia althaamina- altiknulujia walqanuna.

• d/ mahmud salamat eabd almuneim alsharifi, jarimat alaintiqam al'iibahii eabr tiqniat altazyif aleamiq (Deep fakes) walmaswuwliat aljinayiyat eanha, bahth manshur fi majalat alhuquq lilbuhuth alqanuniat walaiqtisadiati, jamieat al'iiskandariat, kuliyat alhuquqi, aleadad al'uwla, yuliu 2022.

• da/ wala' muhamad mahrus alnaaghi, wada/ yasir muhamad mahrus alnaaghi, 'iidrak mustakhdimi mawaqie altawasul aliajtimaeii litahdidat altazyif aleamiq (Deep fakes) waealaqatih bialaistikhdam alamin litilk almawaqiei, bahth manshur fi majalat aleilmiat libuhuth alsahafati, jamieat alqahirati, kuliyat al'iielami, aleadad alraabie waleishrun aljuz' althaalithi, yulyu/ disambir 2022m.

4: altaqarir:

• dalil altazyif aleamiq alsaadir ean albarnamaj alwatanii lildhaka' alaistinaeiu, al'iimarat alearabiat almutahidati, yuliu sanat 2021m.

• aldhaka' alaistinaeiu wamakhatir altazyif aleamiqi, taqrir dawriun yasdur ean markaz almaelumat wadaem aitikhadh alqarar altaabie limajlis alwuzara' almisrii, nushir bitarikh 25 mars 2023.

فهـــرس الموضوعـــات

أهمية البحث: ٢٦٧٥
إشكالية البحث وأهدافه: ٢٦٧٥
منهج البحث: ٢٦٧٦
خطة البحث: ٢٦٧٦
المبحث الأول ماهية التزييف العميق (DEEP FAKE) وسماته ٢٦٧٨
المطلب الأول ماهية التزييف العميق (DEEP FAKE) ٢٦٧٩
المطلب الثاني سمات التزييف العميق (DEEP FAKE) ٢٦٨٤
المبحث الثاني مخاطر التزييف العميق (DEEP FAKE) ٢٦٨٧
المطلب الأول المخاطر السياسية والأمنية للتزييف العميق ٢٦٨٨
المطلب الثاني المخاطر الاقتصادية والاجتماعية للتزييف العميق (DEEP FAKE) ٢٦٩١
المبحث الثالث الجوانب القانونية للتزييف العميق (DEEP FAKE) ٢٦٩٥
المطلب الأول المواجهة التشريعية لتقنية التزييف العميق (DEEP FAKE) ٢٦٩٦
المطلب الثاني أركان جريمة التزييف العميق (DEEP FAKE) ٢٧٠١
المطلب الثالث العقوبة المقررة لجريمة التزييف العميق (DEEP FAKE) ٢٧١٩
الخاتمة: ٢٧٣٠
أولا: نتائج البحث: ٢٧٣٠
ثانيا: التوصيات والاقتراحات: ٢٧٣٢
قائمة المراجع: ٢٧٣٥
REFERENCES: ٢٧٣٩
فهـــرس الموضوعـــات ٢٧٤٢