***Dirasat*: Shari'a and Law Sciences, Volume 53, No. 4, 2026, 13808**

Deanship of Scientific Research

The Extent of Criminal Response to Deepfake Under the Jordanian Cybercrime Law No. 17 of 2023: A Comparative Analytical Study

***Ali Ahmad Abed Alzubi*[1]*, *Haytham Faleh Abed Shehab*[2]**

[1]Department of Law, Faculty of Law, Al-Balqa Applied University, Jordan

[2]The National Center for Human Rights, Amman, Jordan

Received: 24/11/2025
Revised: 22/12/2025
Accepted: 11/3/2026
Published: 8/4/2026

* *Corresponding author:*
alialzubi@bau.edu.jo

Citation: Alzubi, A. A. A., & Shehab, H. F. A. (2026). The Extent of Criminal Response to Deepfake Under the Jordanian Cybercrime Law No. 17 of 2023: A Comparative Analytical Study. *Dirasat: Shari'a and Law Sciences*, *53*(4), 13808. https://doi.org/10.35516/Law.2026.13808

© 2026 DSR Publishers/ The University of Jordan.

This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY-NC) license https://creativecommons.org/licenses/by-nc/4.0/

Abstract

Objectives :This study examines the emerging phenomenon of deepfake crimes associated with artificial intelligence and evaluates how the Jordanian Cybercrime Law No. 17 of 2023 addresses them.

Methods :The study adopts an analytical approach by presenting and analyzing doctrinal opinions and applying general and specific legal provisions to the crime of deepfake.

Results :The findings indicate that Arab criminal laws, including Jordanian legislation, have not established explicit legal provisions that regulate the use of deepfake technology. They also fail to address the responsibility of entities producing or operating this technology. Consequently, both the criminal acts and the role of service providers remain insufficiently regulated. Preventive and remedial measures are largely absent, unlike European and Chinese legislation, which explicitly criminalize such acts and regulate preventive procedures.

Conclusions :The study recommends introducing a specific criminal provision in the Jordanian Cybercrime Law stating: "Without prejudice to any more severe penalty stipulated under any other law, anyone who uses deepfake technology with the intent to commit any crime stipulated in this law or any other punishable offense shall be punished by imprisonment for a period of six months to three years and a fine of not less than 2,000 JOD and not exceeding 5,000 JOD, or both." It also recommends obligating entities producing and operating this technology, including service providers, to implement safeguards preventing misuse and to report deepfake-related activities to the authorities..

Keywords:Criminal response, deepfake crime, artificial intelligence, cybercrime

مدى المواجهة الجنائية للتزييف العميق في قانون الجرائم الإلكترونية الأردني رقم 17 لسنة 2023: دراسة تحليلية مقارنة

***علي أحمد عبد الزعبي*[1]*، هيثم فالح عبد شهاب [2]**

[1]قسم القانون، كلية الحقوق، جامعة البلقاء التطبيقية، الأردن.

[2]المركز الوطني لحقوق الإنسان، عمان، الأردن.

ملخّص

الأهداف: هدفت الدراسة إلى تركيز الضوء على ظاهرة حديثة من جرائم تقنيات الذكاء الاصطناعي، تسمى التزييف العميق (Deep fake)، لمعرفة مدى مواجهتها من قبل المشرع الأردني في قانون الجرائم الإلكترونية رقم 17 لسنة 2023.

المنهجية: تم الاعتماد في الدراسة على المنهج التحليلي من خلال طرح الآراء الفقهية وتحليلها، بجانب تطبيق نصوص القانون العامة والخاصة على جريمة التزييف العميق (Deep fake).

النتائج: توصلت الدراسة إلى أنّ التشريعات الجنائية العربية ومنها الأردني، قد أخفقت في إيجاد نصوص قانونية تحُد من استعمالات التزييف العميق، فضلاً عن أنها قد أخفقت في معالجة دور الجهات المنتجة لهذه التقنية، ولهذا فلم يُحَد من تلك الجرائم، ولا من دور مزودي هذه الخدمة. وأيضا غياب ما يتعلق بها من إجراءات وقائية كانت أم علاجية على عكس ما أقرته التشريعات الأوروبية والصينية بالنص صراحةً على تجريم تلك الأفعال، وتنظيم الإجراءات الوقاية بخصوصها.

الخلاصة: توصي الدراسة بضرورة وضع نص تجريمي مستقل في قانون الجرائم الإلكترونية الأردني، تكون صيغته: "مع مراعاة أي عقوبة أشد منصوص عليها في أي قانون آخر، يُعاقب كل من استخدم تقنية التزييف العميق بقصد ارتكاب أي من الجرائم المنصوص عليها في هذا القانون أو أي جريمة معاقب عليها بموجب أي تشريع آخر، بالحبس من ستة أشهر إلى ثلاث سنوات، وبغرامة لا تقل عن 2000 دينار، ولا تزيد على 5000 دينار، أو بكلتا هاتين العقوبتين". كما توصي الدراسة بضرورة إلزام كل الجهات التي تنتج هذه التقنية وتشغلها، بمن فيهم الجهات المزودة لهذه الخدمة؛ بتطبيق إجراءات تحول دون استخدامها السيء، وإبلاغ السلطات عن عمليات التزييف العميق.

الكلمات الدالة: المواجهة الجنائية، جريمة التزييف العميق، الذكاء الاصطناعي، الجرائم الإلكترونية.

المقدمة.

لقد شهد العالم في الآونة الأخيرة تطوراً سريعاً في مجال استخدام تطبيقات الذكاء الاصطناعي، وتعد تقنية التزييف العميق (Deep fake) التي انتشرت مؤخراً من أهم التطورات التكنولوجية التي تعتمد على الذكاء الاصطناعي، بيد أنّ انتشار هذه التقنيات، وبالرغم من كثرة جوانبها الإيجابية، إلا أنها أدت من جانب آخر إلى إفراز جرائم جديدة عن طريق الاستخدام السلبي لهذه التقنيات؛ لأنها كأي منتج يمكن استخدامها كوسيلة لبناء المجتمعات، كما يمكن استخدامها وسيلة لهدمها (النجار، 2024، ص578)، إذ أنّ تقنية التزييف العميق (fake Deep) تمكن المستخدم من اصطناع مقاطع فيديو أو تسجيل مزيف يبدو وكأنه حقيقي، عن طريق جمع صور وبيانات شخصية للمجني عليه، ثم التلاعب بها ومعالجتها عبر أحد تطبيقات الذكاء الاصطناعي (الحكيم، 2025، ص2674).

فتقنية التزييف العميق (Deep fake) لها جوانب إيجابية تتجسد في بعض الاستعمالات النافعة كالإبداع وما يتعلق بالترفيه وبعض جوانب الإعلام والتعليم، ومجالات أخرى، ويقابل ذلك جوانب سلبية فيما قد يستغله أصحاب النفوس الضعيفة وذوي النزعة الإجرامية؛ كوسيلة فاعلة في ارتكاب جرائم تسمى "جرائم التزييف العميق Deepfake Crimes " (مغايرة، 2024، ص129).

أهمية البحث.

تكمن أهمية هذا البحث في معالجة أحد أهم تطبيقات الذكاء الاصطناعي التي انتشرت في الآونة الأخيرة، فكانت تقنية التزييف العميق (Deep fake) من الظواهر الإجرامية المستحدثة في مجال العلم الجنائي، ومثار نقاش فقهي وقانوني، خاصة بسبب الآثار السيئة التي نجمت عنها على كافة المستويات السياسية والاجتماعية والاقتصادية والأمن المجتمعي والأمن الوطني للدول.

إشكالية البحث وتساؤلاته.

تكمن مشكلة هذا البحث في بيان ما مدى انطباق النصوص الواردة في قانون الجرائم الإلكترونية الأردني رقم 17 لسنة 2023 على أفعال التزييف العميق التي تشكل اعتداءً على الحقوق أو المصالح الجديرة بالحماية الجنائية؟

ويتفرع عن هذا التساؤل عدد من التساؤلات الفرعية من أبرزها:

1. ما مفهوم تقنية التزييف العميق، وما خصائصها؟ وما مخاطرها؟
2. هل العقوبات الجزائية الواردة في النصوص الحالية الأردنية كافية ومتناسبة مع جسامة الأفعال الإجرامية الناتجة عن استخدام تقنيات التزييف العميق؟
3. هل نص المشرع الأردني على جريمة الاستخدام غير المشروع لتقنية التزييف العميق كجريمة مستقلة بذاتها؟ أم من الأنسب إفرادها بنصٍ تجريمي مستقل؟ أم اعتبار استخدام هذه التقنية ظرفاً مشدداً لعقوبات الجرائم الإلكترونية أو الجرائم التي ترتكب بواسطتها، بوصفها وسيلة من وسائل ارتكاب الجريمة؟

أهداف البحث.

يسعى هذا البحث إلى:

1. بيان تعريف تقنية التزييف العميق، وتحديد خصائصها ومخاطر استخدام هذه التقنية.
2. تحديد مدى تناسب وكفاية العقوبات الجزائية الواردة في النصوص الحالية الأردنية مع جسامة الأفعال الإجرامية الناتجة عن استخدام تقنيات التزييف العميق.
3. بيان مدى نص المشرع الأردني على جريمة الاستخدام غير المشروع لتقنية التزييف العميق كجريمة مستقلة بذاته، أم من الأنسب إفرادها بنصٍ تجريمي مستقل، أم اعتبار استخدام هذه التقنية ظرفاً مشدداً لعقوبات الجرائم الإلكترونية أو الجرائم التي ترتكب بواسطتها، بوصفها وسيلة من وسائل ارتكاب الجريمة.

منهجية البحث.

اعتمد البحث على كُلٍّ من المنهج التحليلي، والمنهج المقارن؛ من خلال عرض النصوص القانونية الجنائية في التشريعات الأردنية والمقارنة وتحليلها والمقارنة بينها، للوصول إلى النتائج والتوصيات التي تلقي الضوء على أوجه القصور والنقص بالنسبة للاستخدام غير المشروع لتقنية التزييف العميق في هذه التشريعات، وتقديم الاقتراح للمشرع الأردني حيالها.

خطة البحث.

سيتم تناول البحث من خلال بيان النطاق التعريفي لجريمة التزييف العميق (**Deep fake**) (المبحث الأول)، ومن ثم بيان النطاق المضوعي لجريمة التزييف العميق (**Deep fake**) (المبحث الثاني).

المبحث الأول

النطاق التعريفي لجريمة التزييف العميق (Deep fake)

أدى تطور الذكاء الاصطناعي إلى إيجاد تقنية التزييف العميق (Deep fake) بحيث يتمكن الإنسان باستخدام هذه التقنية من خلال 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 نشأة لها عام 2017 حيث قام بعض الأفراد باصطناع فيديو إباحي لنجمة من نجمات هوليوود (أبو الوفا، 2025، ص6).

وبناء على ذلك، فإن بيان النطاق التعريفي المتعلق بجريمة التزييف العميق يستوجب منا تقسيم هذا المبحث إلى مطلبين، نتناول في الأول بيان مفهوم التزييف العميق (Deep fake)، وفي المطلب الثاني نركز على مخاطر التزييف العميق (Deep fake).

المطلب الأول

مفهوم التزييف العميق (Deep fake)

يساعد التعريف الشامل لجريمة التزييف العميق على فهمها وتحديد أركانها ووضع الحلول القانونية اللازمة للحد من ارتكابها، ومنع وقوعها، ويتألف التزييف العميق من مصطلحين اثنين أولهما العميق (Deep)، الذي يشير إلى برامج ذكاء اصطناعي تستخدم لهذا الغرض، وهو ما يسمى بنموذج التعليم العميق (Model Deep Learning)، وثانيهما التزييف (**fake**)، والذي يعني تزييف حقيقة الواقع، كما أنّ مصطلح "التزييف العميق" يعني استخداماً غير شرعي لتقنية التعليم العميق (مغايرة، 2024، ص133).

لذلك سيتم الحديث عن مفهوم التزييف العميق من خلال النقاط التالية:

أولاً: تعريف التزييف العميق (Deep fake**).**

تعددت التعريفات الفقهية للتزييف العميق، فعرفه أحدهم بأنه: "المصطلح الذي يشير للمقاطع المرئية المُعالَجَة، أو يشير لصورة مُعَدَّلَة لأي شخص ظهر في الفيديو أو لصوته، حتى يبدو كأنه حقيقي" (محرم، 2022، ص2528)، كما عرفه آخر بأنه: "عبارة عن نسخة متطرفة ملفقة وهمية من بيانات سمعية وبصرية تم التلاعب بها من خلال أحد تطبيقات الذكاء الاصطناعي المعدة لذلك، والذي يعني التقول على شخص بشيء لم يقله بواسطة تقنيات تكنولوجية حديثة" (الشريف، 2022، ص369).

وعرفه آخر بأنه: "نوع من التقنية تستعمل الذكاء الاصطناعي لخلق محتوى مزيف يبدو وكأنه حقيقي، عادة ما يتم استخدامها لخلق فيديوهات أو صور تظهر أشخاصاً أو أحداثاً أو أصواتاً وتعابير وجوه تم إنشاؤها بواسطة الكمبيوتر بطريقة تجعلها تبدو وكأنها حقيقة" (أبو العلا، 2024، ص487)، وورد في تعريفه أيضاً أنه: "التقنية التي تجمع بين التزييف (fakes) وتقنية الذكاء الاصطناعي (Learning Deep) المستخدمة في تكوين وإنتاج صورة أو مقطع فيديو أو صوت لشخص غيّر وجهه أو جسده بتقنية رقمية، حتى يظهر كشخص غيره، أو كأن يقوم بفعل محدد، كما تستخدم هذه التقنية في خلق أخبار كاذبة ومحاولة خداع الناس والتسبب بأذى للبعض" (البيومي، 2023، ص831-ص832).

أما البرلمان الأوروبي فوصفه بأنه: "وسائط متنوعة كأن تكون صوتية، أو وسائط بصرية معدلة، أو زائفة فتظهر حقيقية، وتظهر شخصا ما أو أكثر، بحيث يظهرون أنهم يقولون شيئا أو يفعلونه، لكنهم لم يقولوا ذلك ولم يفعلوه إطلاقاً، ثم بعد ذلك يجري انتاجه بوسائل تستخدم تقنية الذكاء الاصطناعي، مثل التعليم التلقائي وكذلك التعليم العميق" (مغايرة، 2024، ص133).

يمكن لنا من خلال مطالعة هذه التعريفات أن نعرف التزييف العميق بأنه: "شكلٌ من أشكال استخدام تقنية الذكاء الاصطناعي وتطبيقاته التي تصنع محتوى سواء أكان رقمياً أو صوتياً أو كلا المحتويين مجتمعين للشخص الواحد، وذلك بمعالجة الصور والفيديوهات والتسجيلات وتحويلها إلى فيديو جديد بحيث يبدو حقيقياً، غير أنه مزيف يخالف الواقع في المحتوى والمضمون".

ثانيا: نشأة التزييف العميق (Deep fake**) وكيفية عمله.**

يمثل مصطلح "التزييف العميق" (Deepfakes)، الذي ظهر عام 2017، ظاهرة حديثة نسبياً في مجال الوسائط التركيبية، تُنتج هذه الوسائط باستخدام تقنيات التعلم الآلي لإنشاء محتوى صوتي أو صور أو فيديوهات أو نصوص معدلة أو تركيبية بالكامل، أو حتى بث مباشر. في البداية، اقتصر مفهوم التزييف العميق على دوائر تقنية محددة، ثم اندمج تدريجياً تحت مظلة أوسع هي الوسائط التركيبية المولدة بالذكاء الاصطناعي (Sandoval et al., 2024, P 41). حيث قام أحد الأشخاص بإنشاء حساب في (Reddit)، وكان يحمل الحساب اسم (Deep fake)، وقام المستخدم بإنشاء مقطع فيديو إباحي لإحدى نجمات هوليوود، وبعد ذلك أزيل هذا الحساب من الموقع سالف الذكر، وفي سنة 2022 قامت شركة سامسونج بإضافة نظام في هواتفها يمكن المستخدمين من إنشاء مقاطع مرئية باستخدام الصور الثابتة، وظهر في سنة 2023 تطبيق يمكن المستخدم من إنشاء

فيديوهات لموتى يتحركون، ويتحدثون كالأحياء (أبو سيف، 2025، ص1646؛ مغايرة، 2024، ص130)، ومنذ ذلك الحين إلى يومنا هذا ازداد صنع ونشر الفيديوهات والصور المزيفة عبر تقنية التزييف العميق (fake Deep).

يمثل التزييف العميق (Deep fake) استخدام تطبيق من تطبيقات الذكاء الاصطناعي يُعْرف بنموذج التعليم العميق Model Deep(Learning)، إذ يمكننا هذا الاسم من الوقوف على أبرز الخصائص والسمات المتعلقة بهذا النموذج، والمسمى بالتعليم الذاتي أو التلقائي، وهو المتخصص بخلق صور إضافة إلى مقاطع الفيديو المرئية والصوتية "Voice Cloning or Synthetic Voice" للشخص المعني طبق الأصل، مأخوذة من نسخته الأصلية، وهذا يجعل إنتاج صورة مزيفة طبق الأصل ممكنا، لكن بمحتوى مغاير للحقيقة تماما؛ فتبدو حقيقية ومتطابقة مع النسخة الأصلية. وهكذا، نجد أن لدينا فيديو الشخص المعني بالصوت والصورة، إلا أنها حركات وتصرفات لا تمثل واقع الشخص المعني ولا حقيقته بحال (النجار، 2024، ص582؛ ستين، 2023، ص74).

إن هذا ممكن وعلى وجه الخصوص، من خلال استخدام نوع من الشبكات الذكية والعصبية العميقة، المسماة "شبكات التوليد المعارض" "Generative Adversarial Networks" التي اخترعت من قبل الباحث في شركة جوجل إيان قودفلو "Goodfellow Ian" عام 2014، وهي عبارة عن شبكتين متضادتين تتعلمان من بعضهما البعض من خلال التنافس بينهما، فالشبكة الأولى تسمى "المميز" (Discrriminator) والشبكة الثانية تسمى "المولد" (Generator)؛ حيث تقوم الشبكة الأولى بالتمييز (بين أي بيانات مزيفة وحقيقية لذلك المحتوى، في حين تحاول الشبكة الثانية إنشاء واقع بيانات أشد إقناعا بهذا الواقع، إلى حد تَعَذُّر تمييز الشبكة الأولى "المميز" لها عن أي بيانات حقيقية ذات علاقة، وتمتد عملية التنافس بين الشبكة الأولى والثانية، إلى أن تتمكن الشبكة الثانية "المولد" من إيجاد محتوى ربما يتعذر تمييزه عن حقيقة المحتوى بواسطة الشبكة الأولى "المميز" (مغايرة، 2024، ص131-ص132).

ثالثاً: خصائص التزييف العميق (Deep fake)

للتزييف العميق عدد من الخصائص نذكر أهمها كما يلي:

1. **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 (العبيدي، 2022، ص31).
2. **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 الآثار سياسية أو اقتصادية أو أمنية (أبو سيف، 2025، ص1662؛ الحكيم، 2025، ص2685).
3. **التزييف سلوك يعتمد على معالجة البيانات:** يعتبر تداول الصور والفيديوهات والتسجيلات 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 وإنتاج فيديو أو تسجيل فيديو جديد مزيف يخالف الأول في المحتوى والموضوع، ويخالف الواقع، وبعد ذلك يشارك هذا المنتج مع الآخرين، بهدف تهديد المجني عليه أو التشهير به، أو إشاعة أخبار كاذبة عنه، أو غيرها من الأهداف (أبو العلا، 2024، ص488-ص489؛ أبو الوفا، 2025، ص11).
4. **التزييف العميق صعب الاكتشاف:** لا يحتاج إنتاج الفيديوهات أو التسجيلات المزيفة عبر تقنية التزييف العميق إلى الأساليب والطرائق التقليدية من استعمال العنف مثلاً، وإنما يستلزم الحاسب الآلي وشبكة الإنترنت فقط، ولذلك يصعب اكتشافه، لأنه يتم في الفضاء الإلكتروني، فلا يترك أثراً خارجياً مادياً يمكن الاستفادة منه في ملاحقة مرتكبه وضبطه، ويضاف إلى ذلك أيضاً أنه ذو طبيعة فنية يحتاج كشفها إلى المتخصصين، وفي الوقت نفسه يتسم بسهولة الارتكاب، فوسيلة 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 حقيقياً، ولا يمكن كشفه لا سيما بالنسبة للأفراد العاديين (البيومي، 2023، ص841-ص842؛ النجار، 2024، ص585).

المطلب الثاني

مخاطر التزييف العميق (fake Deep)

دراسة مخاطر تقنية التزييف العميق تستلزم منا تناولها في عدة نقاط، على النحو التالي:

أولاً: المخاطر السياسية للتزييف العميق (Deep fake).

في المجال السياسي، يتم تسخير تقنية التزييف العميق بشكل متزايد لنشر المعلومات المضللة، سواء من قبل المتطرفين أو الجهات الفاعلة، ففي عام 2020 نشرت صفحة صهيونية على فيسبوك مقاطع فيديو لأشخاص مُولّدين بتقنية التزييف العميق، زعموا أنهم يساريون متحدون الآن خلف رئيس الوزراء الإسرائيلي المحافظ نتنياهو. كما أنتجت جماعة الضغط التقدمية "RepresentUS" مقطع فيديو مزيفًا لكيم جونغ أون يتباهى فيه بانهيار الديمقراطية الأمريكية (Broinowski and Martin, 2024, P11 ,).

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 2019، ولكن قام أحد الأشخاص بتركيب وجه الرئيسة على وجه المدمنة (مغايرة، 2024، ص140؛ محرم، 2022، ص2534).

كما أن تقنية التزييف العميق (fake Deep) 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 مواطنها، 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 (الحكيم، 2025، ص2689). حيث أظهر تقرير لمجموعة من الباحثين في جامعة أكسفورد أن 25٪ من المحتوى السياسي الذي تم نشره حول الانتخابات الفرنسية كان مزيفاً ومضللاً، ولا يمت إلى الحقيقة بأية صلة (أبو العلا، 2024، ص492)، وهذا يدل على حجم استغلال تقنية التزييف العميق في العمليات الانتخابية في مختلف الدول.

ثانياً: المخاطر الأمنية للتزييف العميق (Deep fake).

تعد تقنية التزييف العميق أخطر 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 2022 يأمر جنوده بإلقاء أسلحتهم، والاستسلام في القتال ضد الغزو الروسي، فنشرت الحكومة الأوكرانية بياناً رسمياً أوصت فيه جنودها بتوخي الحذر من الفيديوهات المفبركة بتقنية التزييف العميق، والتي تنشر في شبكات الإنترنت، وتستهدف إحداث البلبلة والتفريق في صفوف الجيش (البيومي، 2023، ص837؛ النجار، 2024، ص588).

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 (ستين، 2023، ص111)، في هذا الإطار كانت مخاطر التزييف العميق على الأمن القومي والعمليات الانتخابية هي أساس نقاشات خلال جلسة استماع للجنة الاستخبارات في مجلس النواب الأمريكي، إذ كانت لهذه التقنية آثار سيئة على انتخابات 2020 (محرم، 2022، ص2534).

ثالثاً: المخاطر الاقتصادية للتزييف العميق (Deep fake).

تُشكّل تقنية التزييف العميق، المدعومة بتقنيات متطورة للتعلم العميق والرؤية الحاسوبية، مخاطر جسيمة على عمليات صنع القرار في الشركات. فمن خلال توليد محاكاة واقعية للغاية لمواقف وأفراد وأحداث حقيقية، تُشكّل هذه التقنية تحديًا لقدرة المؤسسات على التمييز بين المحتوى الأصلي والوسائط المُعدّلة. وحتى أنظمة الكشف المتقدمة قد تُخدع بقدرة تقنية التزييف العميق على إنتاج محتوى مُختلق فائق الواقعية (Vecchietti et al ,2025, P 10).

كما يعد استعمال تقنية التزييف العميق في الاحتيال مصدر قلق لدى أصحاب الأموال، وليس من قبيل المصادفة إذن أن الجرائم الإلكترونية المدعومة بتقنية التزييف العميق آخذة في الازدياد. تشير تقديرات المنتدى الاقتصادي العالمي إلى أن تقنية التزييف العميق استُخدمت في 66% من الجرائم الإلكترونية التي ارتُكبت خلال عام 2022. وقد استخدم مجرمون، في عام 2021، تسجيلات صوتية مُزيّفة بتقنية التزييف العميق لمدير تنفيذي شركة لإقناع مدير فرع بتحويل 35 مليون دولار أمريكي إلى حساباتهم. في عام 2022، حذّر مكتب التحقيقات الفيدرالي من أن قراصنة

الإنترنت كانوا يرتدون أقنعة مُزيّفة بتقنية التزييف العميق في مقابلات العمل الإلكترونية في مجال أمن التكنولوجيا للوصول إلى أنظمة حساسة. في عام 2023، استخدم مُعلنون مُخالفون سلسلة من عمليات التزييف العميق للمشاهير: فقد باع مُزوّر لشخصية توم هانكس خططًا لطب الأسنان دون موافقته؛ ورفعت سكارليت جوهانسون دعوى قضائية ضد شركة ناشئة لتزييفها بتقنية التزييف العميق في ترويج لتطبيق ذكاء اصطناعي؛ واستخدم إعلان تجاري أسترالي تسجيلًا مُزيّفًا رديء الصوت لوزير الخزانة الفيدرالي جيم تشالمرز للترويج لمنصة تداول وهمية (Broinowski and Martin, 2024). كذلك تمكن مجرمو الإنترنت من OGHG خداع أحد المتخصصين في الشؤون المالية ودفعه إلى دفع 25 مليون دولار أمريكي، وذلك بانتحال شخصية المدير المالي لشركة متعددة الجنسيات عبر مؤتمر فيديو. وفي هونغ كونغ أيضاً، استخدم الجناة ثماني بطاقات هوية مسروقة لتقديم 90 طلب قرض و54 عملية تسجيل حسابات مصرفية بطريقة احتيالية خلال ثلاثة أشهر (Vecchietti et al., 2025, P12).

كذلك 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 (الشريف، 2022، ص372)، 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 (العبيدي، 2022، ص104).

رابعاً: 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 النيل من الضحية وإذلالها والانتقام منها (ستين، 2023، ص132؛ البيومي، 2023، ص842)، وقد يستتبع إنتاج مقاطع الفيديوهات الإباحية الابتزاز الجنسي أو المالي أيضاً، حيث يطلب الجاني من الضحية لعدم نشر الفيديو إقامة علاقة جنسية غير مشروعة معها، وقد يطلب منها مبلغاً مالياً (مغايرة، 2024، ص136؛ الشريف، 2022، ص373-ص374).

من 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 (محرم، 2022، ص2535). ونظرًا لإمكانية التلاعب بسهولة بالتسجيلات الصوتية والمرئية لتغيير الواقع، فقد بات التمييز بين الأدلة الحقيقية والمحتوى المُفبرك أكثر صعوبة. وتؤثر هذه المشكلة بشكل مباشر على نزاهة التحقيقات الجنائية، وتُعرّض التحقيقات لخطر نتائج غير عادلة، كتبرئة المُذنبين أو إدانة الأبرياء ظلمًا. ويمكن أيضًا استخدام تقنية التزييف العميق لتلفيق الأدلة ضد الادعاء، والتشكيك في شهادة الشهود، وبناء روايات كاذبة، مما يعقد قدرة جهات إنفاذ القانون على تجميع رواية موثوقة للأحداث (Loovens and Tinmaz, 2025, P32).

بالإضافة 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، إذ قد يترتب على سوء استعمال هذه التقنية انتشار خطاب الكراهية، والتنمر وأعمال الشغب، وإحداث بلبلة في المجتمع (الشريف، 2022، ص373).

المبحث الثاني

النطاق الموضوعي لجريمة التزييف العميق (Deep fake)

مع استمرار الابتكار التكنولوجي في تجاوز التشريعات في اقتصاد اتصالات الذكاء الاصطناعي، تتجه منصات التكنولوجيا الكبرى إلى تنظيم عمليات التزييف العميق ذاتيًا. وتحظى هذه الإجراءات بدعم مؤسسي، على الرغم من سجل الشركات المشكوك فيه في مجال الحوكمة الذاتية (Broinowski and Martin, 2024, P17). إن إنتاج ونشر ووجود تقنية التزييف العميق يمثل في حد ذاته تحدياً لأنظمة العدالة الجنائية في العديد من الولايات القضائية (Sandoval et al., 2024 , P44).

تقنية التزييف العميق كغيرها من تطبيقات الذكاء الاصطناعي لها استخدامات إيجابية وسلبية، وأن استخدامها السلبي يشكل جريمة من الجرائم؛ لأن فيه اعتداء على حق الأفراد في الخصوصية والكرامة؛ ولأنه قد يشكل خطراً كبيراً 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، وقبل ذلك يجب بيان موقف التشريعات هذه الجريمة.

بناء على ذلك، فإن دراسة النطاق الموضوع لجريمة التزييف العميق تستوجب منا تقسيم هذا المبحث إلى مطلبين، نتناول في المطلب الأول موقف التشريعات من جريمة التزييف العميق (Deep fake)، بينما نخصص المطلب الثاني لأركان جريمة التزييف العميق (Deep fake).

المطلب الأول

موقف التشريعات من جريمة التزييف العميق (Deep fake)

تعد المواجهة التشريعية من أهم أدوات الردع عن الاستخدام السلبي لتقنية التزييف العميق (Deep fake) والتصدي لها والحد من حالات الإفلات من العقاب العادل الذي يناسب جسامة الفعل، وتعتبر جمهورية الصين الشعبية من أوائل الدول التي أصدرت عدداً من التشريعات والأحكام التي تنظم الذكاء الاصطناعي عامة، وتقنيات التزييف العميق خاصة؛ إذ في نهاية سنة 2022 أصدرت إدارة الأمن المعلوماتي متعاونة مع وزارة الصناعة والتكنولوجيا ومع وزارة الأمن العام في الصين، النظام المسمى "بنظام أحكام إدارة خدمات معلومات الإنترنت للتزييف العميق"، والذي يضُم (25) مادة كلها تخص استخدام تقنية التزييف العميق، التي أصبحت سارية المفعول في 10 يناير 2023، وكان أهَمِّهِ ما ورد في المادة (6) منه ونصها "لا يحق لأي منظمة أو فرد استعمال الإنترنت لتزييف عميق في إنتاج أو نسخ أو نقل أو نشر معلومات محظورة وفق القوانين السارية واللوائح الإدارية، كتعريض الأمن الوطني والمصالح الوطنية لأي خطر، أو الإضرارٍ بصورة الوطن، أو انتهاك المصلحة العامة، أو الإساءة للنظام الاقتصادي أو الاجتماعي، أو حقوق الآخرين ومصالحهم القانونية، أو نشر أخبار كاذبة"، كما نصَّ هذا النظام على ما يقع على عاتق مزودي خدمة تقنية التزييف العميق من التزامات، ومن أهمها مسؤوليتهم عن تأمين أمن أي معلومات وسلامتها وكذلك ما يخص المستخدمين من بيانات وما يتعلق بتسجيل أسماءهم الحقيقية، ومنع الاحتيال (المادة 7 من النظام)، كذلك ألزم النظام في المادة (9) منه مزودي الخدمة بالقيام ما يضمن التحقق من هوية مُسْتَخْدِمي تقنيات التزييف العميق وبياناتهم، وفي المادة (11) منه تم إلزام مزودي الخدمة بعمل إجراءات وقتية عند كشف محتوىً مزيف يتعارض مع أحكام القانون الصيني، ويتألف ذلك من عدة تدابير يمكن بواسطتها دحض ما جاء في المحتوى المزيف، وحفظ سجل خاص به، مع إبلاغ السلطات المعنية (النجار، 2024، ص591-ص592).

بالمقابل، على مستوى الاتحاد الأوروبي؛ فقد طرح الاتحاد الأوروبي عن طريق المفوضية الأوروبية في شهر ابريل من سنة 2021 إطاراً قانونياً تنظيمياً كان مقترحاً من المفوضية نفسها، يخص معالجة مخاطر تقنية الذكاء الاصطناعي، والذي تم عرضه للمناقشة في جلسة البرلمان الأوروبي بتاريخ 21 يونيو سنة 2023؛ ونتيجة لذلك اعتمد الاتحاد الأوروبي اللائحة رقم 2024/1689 سُميت "قانون الذكاء الاصطناعي" في نهاية مايو 2024، وفي 12 يوليو 2024 نشر قانون الذكاء الاصطناعي في الجريدة الرسمية للاتحاد الأوروبي، ودخل حيز النفاذ في جميع الدول الأعضاء السبع والعشرين في الاتحاد الأوروبي اعتباراً من 1 أغسطس 2024، وأن يبدأ تطبيق غالبية أحكامه في 2 أغسطس 2026، على أن تدخل الالتزامات المدرجة في القانون حيز التنفيذ تدريجياً على مدى جدول زمني لتسري معظم الأحكام بحلول منتصف عام 2027 (أبو يوسف، 2025، ص1646-1647).

حيث يتألف قانون الذكاء الاصطناعي للاتحاد الأوروبي من 180 فقرة و113 مادة، ويتبع نهجاً قائماً على المخاطر لتنظيم دورة حياة الأنواع المختلفة من أنظمة الذكاء الاصطناعي بالكامل، وقد تضمن القانون عقوبات هي عبارة عن غرامات مالية قد تبلغ 35 مليون يورو، أو ما يصل إلى 7% من مجمل المبيعات السنوية على مستوى العالم، أيهما أعلى، وذلك لمواجهة عدم الامتثال لأحكام القانون، كما وينص القانون على منهجية قوية عند تقدير المخاطر في تناول أنظمة الذكاء الاصطناعي "عالية المخاطر"، والتي تشكل خطورة كبيرة على صحة الأشخاص أو سلامتهم أو حقوقهم الأساسية، حيث يتعين على هذه الأنظمة اتباع إجراءات تقييم المطابقة قبل طرح هذه الأنظمة في سوق الاتحاد الأوروبي (أبو يوسف، 2025، ص1648).

كما تنص المادة (50) من هذا القانون على مجموعة من الالتزامات بالشفافية التي تقع على عاتق الموردين والناشرين لأنظمة الذكاء الاصطناعي، منها ما يتعلق بمواجهة التزييف العميق باستخدام أنظمة الذكاء الاصطناعي، وهي على النحو التالي:

1. الالتزام بوضع علامة يمكن قراءتها بوضوح على مخرجات أنظمة الذكاء الاصطناعي المخصصة للأغراض العامة والتي تولد محتوى اصطناعي من الصوت أو الصورة أو الفيديو أو النص، تفيد أنه مزيف أي ما تم إنشاؤه أو التلاعب به بواسطة أنظمة الذكاء الاصطناعي غير حقيقي.
2. الالتزام باحترام حق الأشخاص في الخصوصية، وكافة القيود المنصوص عليها في الاتحاد الأوروبي لحماية الحق في الحياة الخاصة.
3. التزام القائمين على نشر نظم الذكاء الاصطناعي بالإشارة إلى أن هذا النظام يقوم بإنشاء أو معالجة الصورة أو المحتوى الصوتي، أو أي فيديو يمكن أن يشكل جريمة التزييف العميق، إلى محتوىً أنشأه أو عالجه الذكاء الاصطناعي (المادة 50 من قانون الذكاء الاصطناعي الأوروبي رقم 1689 لسنة 2024).

يستثنى من هذه الالتزامات عندما يكون الاستخدام مسموحاً به بموجب القانون لأغراض منع الجريمة أو اكتشافها أو لأغراض التحقيق القانوني فيها، أو كل ما يخص ملاحقة المتورطين فيها قضائيا، أو إذا كان المحتوى يشكل جزءا من عمل آخر أو برنامج إبداعي أو برنامج فني أو خيالي، أو ما شابه ذلك؛ فتتمتع تلك الالتزامات بالشفافية بكيفية ملائمة لا تتعارض مع عرض ذلك المنتج أو التمتع به، ويترتب على الإخلال بتلك الالتزامات المتعلقة بالشفافية أن يتم توقيع عقوبة الغرامة المالية الإدارية التي تصل إلى 15 مليون يورو على القائمين بالنشر أو الموردين أو المشغلين لأنظمة الذكاء الاصطناعي أو نسبة 3% من إجمالي مبيعات الشركة السنوية في جميع أنحاء العالم أيهما أكبر (الفقرة الرابعة من المادة 99 من قانون الذكاء الاصطناعي الأوروبي رقم 1689 لسنة 2024) (اللمعي، 2025، ص113-ص114؛ أبو يوسف، 2025، ص1651).

يتضح لنا مما سبق؛ أن المشرع الصيني والأوروبي لم يكتفيا بأيٍّ من القوانين التقليدية أو القوانين السيبرانية؛ لمواجهة جريمة التزييف العميق (Deep fake)؛ إيماناً منهما بقصور تلك القوانين في مواجهة فعالة لتقنية قد تستخدم بشكل سلبي بطريقة لم يسبق لها مثيل، أو رغبة من المشرع في تحديد حجم العقوبات عن جرائم التزييف العميق، فالقانونين يؤديان دوراً مهمًا في تأمين الإجراءات الوقائية والجزائية التي تمنع إنتاج التزييف العميق لأي غرض إجرامي، بتفعيل دور أي مزود للخدمة، وإلزام الجهة المنتجة بعمل أي إجراءات ضرورية من شأنها أن تكشف التزييف، كما يُمَكِّنْ القانونان الصيني والأوروبي تحقيق ردع سبل هذه الجريمة، عن طريق الإشارة إلى جرائم وعقوبات مترتبة على استخدام التقنية السلبي.

بالنسبة للدول العربية؛ 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، إذ نجد أن المشرع الأردني أصدر قانون الجرائم الإلكترونية الأول سنة 2010. وكان هذا القانون عاجزا عن مواكبة أي تطورات في مجال تلك الجرائم، لذا أصدر قانوناً جديداً سنة 2015، والمسمى قانون الجرائم الإلكترونية، وتوالت القوانين، إذ في سنة 2023، أصدر المشرع الأردني قانونه الجديد بدل قانون 2015، إذ كان جليًّا قصور الأخير في علاج مختلف الجرائم الإلكترونية، وقد أشار المشرع الأردني في قانونه هذا إلى جريمة التزييف العميق، بطريقة غير مباشرة، فجاء في فقرة القانون الثانية من المادة (20) منه: "ب- يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن (25000) خمسة وعشرين ألف دينار، ولا تزيد على (50000) خمسين ألف دينار كل من استخدم شبكة معلوماتية أو تقنية المعلومات أو نظام المعلومات أو موقعا إلكترونيا أو منصة تواصل اجتماعي لإجراء تركيب أو تعديل أو معالجة على تسجيل أو صورة أو مشهد أو فيديو لما يحرص الشخص على صونه وعدم اظهاره للعامة بقصد التشهير أو الإساءة أو الحصول على منفعة من جراء ذلك".

من الممكن الاعتماد على هذا النص لتجريم بعض أشكال جرائم التزييف العميق، مثل: جرائم الابتزاز المالي، والانتقام الإباحي العميق، لكن هذه المادة المذكورة لا تطال الجرائم الأخرى التي لا تستهدف ما يحرص الشخص على صونه، وعدم إظهاره للعامة، مثل: جرائم زعزعة الاستقرار الأمني للمجتمع (مغايرة، 2024، ص147-ص148).

بالمقابل أصدر المشرع الإماراتي مرسوم بقانون اتحادي إماراتي تحت الرقم 34 لعام 2021 في شأن مكافحة الشائعات المختلفة والجرائم الإلكترونية، وبعد الاطلاع على القانون المذكور؛ نجده يخلو من أي إشارة لجرائم التزييف العميق، لكنه احتوى في بعض مواده، ما يمكن من خلالها تجريم نوعية تلك الجرائم بطريقة أخرى ليست مباشرة؛ حيث تنص المادة (13) من هذا القانون على أنه: "يعاقب بالحبس والغرامة بما لا يقل عن 50000 خمسين ألف درهم، ولا تزيد عن 500000 خمسمائة ألف درهم، أو بإحدى العقوبتين المذكورتين، كل من استعمل تقنية معلومات، أو وسيلة من وسائل تقنية المعلومات، لجمع بيانات شخصية للمواطنين أو المقيمين بالدولة أو معالجة تلك البيانات أو حفظها، بالمخالفة لتشريعات الدولة النافذة"، كذلك من الجرائم المنصوص عليها قانوناً أي جرائم تحريض من شأنها أن تمس أمن الدولة (المادة 23)، وأيضا المادة رقم (24) المتعلقة بترويج إثارة أي فتنة أو إضرار بالوحدة الوطنية، كذلك جرائم الابتزاز أو التهديد بالوسائل الإلكترونية في المادة (42)، كذلك المادة (44) الفقرة الخامسة التي تجرم القيام بأي تعديل أو معالجة على تسجيل أو صورة أو مشهد، بقصد التشهير أو الإساءة إلى شخص آخر.

من ذلك أيضاً المادة (26) من القانون المصري رقم (175) لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات، إذ تنص المادة المذكورة على أنه: "يعاقب بالحبس لمدة لا تقل عن سنتين، ولا تتجاوز خمس سنوات، وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز ثلاثمائة ألف جنيه، أو بإحدى العقوبتين المذكورتين، كل من تعمد استخدام أي برنامج معلوماتي، أو استخدام أي تقنية معلوماتية، تفضي إلى معالجة معلومات أو معطيات شخصية لغيره، بقصد ربطها بمحتوى ينافي الآداب العامة؛ أو لإظهار تلك المعطيات بطريقة تمس ذلك الشخص باعتباره شخصيا، أو بشيء يمس شرفه".

يذكر أنه من التشريعات العربية التي واكبت تطورات التكنولوجيا الحديثة القانون الليبي رقم (5) لسنة 2022 بشأن مكافحة الجرائم الإلكترونية، إذ يعتبر القانون المذكور من التشريعات التي عالجت الاستخدام غير المشروع لتقنية التزييف العميق (Deep fake) بشكل شبه مباشر، إذ تنص المادة (21) من القانون سالف الذكر بأنه ("يعاقب بالحبس لمدة لا تقل عن سنة، كل من مزج بدون أن يصرح له صاحب الشأن كتابيا أو إلكترونيا صورة أو صوتا لأحد الأشخاص أو رَكَّبَها عن طريق استعمال شبكة معلومات دولية، أو بأي وسيلة إلكترونية أخرى، قاصدا إضراراً بالآخرين، إلا إذا كان ذلك مسموحا به في قوانين تنظيم عمل الصحافة وقوانين الحقوق والحريات العامة. أما إذا كان المزج المذكور أو التركيب معمولا مع صور إباحية أو أصوات إباحية، وقام بنشرها على شبكة معلومات دولية، أو بأيّ وسيلة إلكترونية أخرى، فستكون عقوبته السجن لمدة لا تقل عن خمس سنوات".

هنا نرى قصور النصوص العربية التي سبق ذكرها لتجريم أشكال محددة من جرائم التزييف العميق (Deep fake) عن تقديم نصوص قانونية خاصة وشاملة بذلك، ونراها قاصرة عن علاج كل جوانب الاستخدامات المحتملة لتقنية التزييف العميق (Deep fake).

إضافة إلى أن تلك النصوص لم تعالج ما يتعلق بدور شركات إنتاج تقنيات التزييف العميق ولا الحد من جرائمها، ولا ما يتعلق بدور مزودي

الخدمة مثلا، ونلاحظ غياب التفاصيل الدقيقة المتعلقة بتلك الجرائم، وكذلك غياب أي إجراءات وقائية أو علاجية تخصها، كتلك التي جاء بها المشرعون الصينيون والمشرعون الأوروبيون بالنص صراحةً على مكافحة تلك الجرائم.

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 دونه فيلزم أن يكون للفعل المكون للجريمة مظهر خارجي يمكن إدراكه (المجالي، 2023، ص251)، 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 (أحمد، 2021، ص177-ص178؛ اللمعي، 2025، ص116).

لذلك سنفصل في أركان هذه الجريمة على النحو التالي:

أولاً: 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 أثراً أو نتيجةً في العالم الخارجي، وبالإضافة إلى ذلك يجب أن يكون بين السلوك الإجرامي والنتيجة صلة تربطهما، وذلك بأن يكون السلوك سببا في حدوث النتيجة (حسني، 2024، ص586)، وبناءً على ذلك فإن الركن المادي لجريمة التزييف العميق يستوجب تناول هذه العناصر، وذلك على النحو التالي:

1. **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 (نايل، 2020، ص135)، وهذا السلوك يختلف باختلاف الجرائم، وذلك لاعتبارات متعددة نحو: طبيعته والمدة اللازمة لتنفيذه والظروف المسببة له (المجالي، 2023، ص255).

يتمثل 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 (العبيدي، 2022، ص141؛ إبراهيم، 2022، ص172).

فنجد أنّ المشرع الأردني في المادة (20) من قانون الجرائم الإلكترونية قد عبر عن ذلك بقوله: "لأي إجراء يتم بواسطته تركيب أو تعديل، أو أي معالجة لتسجيل أو صورة أو مشهد أو فيديو لما يهم الشخص المعني الحرص عليه وصونه، والامتناع عن إظهاره للغير"، كما نجد أن المشرع الإماراتي قد عبر عن هذا المعنى: "بمعالجة بيانات ومعلومات شخصية للمواطنين أو المقيمين بالدولة"، وعبر عنه المشرع المصري: "بمعالجة معطيات شخصية للغير"، وعلى عكس هذه التشريعات فقد عبر عنه المشرع الليبي: "بمزج أو تركيب صوت أحد الأشخاص أو صورته"، ويعتبر هذا التعبير من أدق التعبيرات، لإفادته المعنى المقصود بصورة كاملة.

2. **النتيجة الإجرامية لجريمة التزييف العميق (Deep fake):** 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 (نايل، 2020، ص146).

ذهب جانب من الفقه إلى أن للنتيجة معنيين: المعنى المادي والمعنى القانوني، وفقاً للمعنى المادي فهو التغيير الملموس الذي يحدث في العالم الخارجي وتدركه الحواس، مثل: الموت في جرائم القتل، وانتقال الحيازة في جرائم السرقة، سواء كان التغيير مادياً أو معنوياً، يصيب المصلحة الخاصة، أو المصلحة العامة (سرور، 2023، ص561)، ويقصد بها وفقاً للمدلول القانوني الاعتداء على المصلحة التي يحميها قانون العقوبات، وذلك إهدارها كاملاً 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 (مغايرة، 2024، ص145-ص146؛ حسني، 2024، ص608).

لذلك نرى أنّ كلا المعنيين وجهان لعملة واحد، حيث إن النتيجة القانونية تحدد النموذج القانوني للجريمة، والتي يجب أن تطابقها النتيجة المادية، وإلا فلا اعتبار لها.

قد اختلف 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 (اللمعي، 2025، ص121؛ القاضي، 2020، ص181).

- الاتجاه الثاني: بينما 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 حقيقياً ولا يتمكن من كشفه إلا المتخصصون (ستين، 2023، ص184؛ سويلم، 2024، ص126).

بناءً على ذلك؛ نجد أنه لا 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 يقل بها أساساً، أو يظهره في حالة الإتيان في ببعض تصرفات لم يأتها، فإذا لم يتم اصطناع الفيديو أو التسجيل وتوقف النشاط مراحله الأولى، أو تم الاصطناع إلا أنه لا يبدو حقيقاً بل مشوهاً ويمكن كشفه، فلا تعتبر الجريمة متحققة؛ وإنما تكون قد توقفت في مرحلة الشروع.

3. **علاقة السببية لجريمة التزييف العميق (**Deep fake**):** تعد علاقة السببية العنصر الثالث من عناصر الركن المادي للجريمة، يقصد بها الرابطة التي تصل بين السلوك الإجرامي والنتيجة الإجرامية، فهي حلقة الوصل بين النشاط والأثر، حتى يمكن القول بأن النتيجة ثمرة للنشاط (نايل، 2020، ص150-ص151؛ أبو الوفا، 2025، ص28).

غير أن أهمية علاقة السببية تقتصر على الجرائم المادية (جرائم النتيجة)، ولا تمتد إلى الجرائم ذات النتيجة الشكلية فقط (جرائم الخطر) (سرور، 2023، ص615)، لذا نرى أنه يترتب على عدم تحقق هذا العنصر انتفاء مسئولية الجاني في الجرائم المادية (جرائم النتيجة) عن جريمة تامة، وإنما يسأل حينئذ عن الشروع في الجريمة، أما في الجرائم الشكلية (جرائم الخطر) فيتحقق الركن المادي بمجرد القيام بالسلوك المجرم دون اشتراط تحقق نتيجة معينة، ولا يتصور فيها الشروع من حيث المبدأ.

بالنسبة للاستخدام غير المشروع لتقنية التزييف العميق (Deep fake) فقد سبق بيان أنها من الجرائم الشكلية (جرائم الخطر) وفقا للاتجاه الأول، وبالتالي لا يستلزم لتحققها 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 الشكلية، فلا يستلزم لتحقيقها علاقة السببية، لأنها تقتصر على جرائم الخطر (الحكيم، 2025، ص2713؛ العبيدي، 2022، ص181)، أما بالنسبة للاتجاه الثاني فيلزم أن يكون بين النتيجة الإجرامية والنشاط الإجرامي علاقة السببية، وذلك بأن يكون الثاني سبباً 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، باعتبار أنّ جريمة التزييف العميق هنا من الجرائم المادية (جرائم النتيجة) (أبو الوفا، 2025، ص33؛ موسى، 2022، ص166).

ثانياً: الركن المعنوي لجريمة التزييف العميق (Deep fake).

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 (سرور، 2023، ص645).

حيث تعد جريمة الاستخدام غير المشروع لتقنية التزييف العميق (Deep fake) من الجرائم العمدية (القصدية)، وقد نصت المادة (20) من قانون الجرائم الإلكترونية الأردني على ذلك بقولها: "...، كأن يكون يقصد منه تشهير أو إساءة أو الحصول على أي منفعة جراء أيّ مما ذكر، كما نص على ذلك المشرع المصري في المادة (26) من القانون رقم (175) لسنة 2018 في شأن مكافحة جرائم تقنية المعلومات، حيث تنص بأنه: "يعاقب ... 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 (سويلم، 2024، ص128).

لما 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 (أبو الوفا، 2025، ص38؛ أحمد، 2021، ص179-ص180)، 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 (العبيدي، 2022، ص196؛ نايل، 2020، ص203-ص204)، وتفصيلهما على النحو التالي:

1. **عنصر العلم:** يقصد بالعلم الحالة النفسية التي تقوم في ذهن الجاني، وجوهرها الوعي بحقيقة الأفعال التي يتكون منها الركن المادي للجريمة، مع توقع النتيجة التي يمكن أن يحدثها النشاط الإجرامي (المجالي، 2023، ص379)، 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 (إبراهيم، 2022، ص194؛ حسني، 2024، ص637).

بناء 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 فعلياً على أرض الواقع، وأنه يقوم بربط البيانات التي حصل عليها بمحتوى مناف للآداب العامة وفقا للتشريع المصري، أو يقوم بمعالجة البيانات بقصد الإضرار بالغير وفقاً للتشريع الليبي، فإذا لم يكن الجاني عالماً 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 (القاضي، 2020، ص181؛ موسى، 2022، ص171).

2. **عنصر الإرادة:** تعد الإرادة العنصر الثاني للقصد الجنائي، ويقصد بها النشاط النفسي الذي يتجه إلى تحقيق غرض معين عن طريق وسيلة معينة (نايل، 2020، ص213)، وهذا العنصر يستلزم الوعي والإدراك لكونه نشاطاً نفسياً، وبالتالي يقتضي العلم بالغرض المراد تحقيقه، والوسيلة التي يستعان بها لتحقيق ذلك الغرض، ويُعد الغرض هدفاً قريبا للإرادة، إذ إن لها هدفاً بعيداً أيضاً، وهو الغاية، التي تتمثل في إشباع الحاجة (حسني، 2024، ص642).

فعنصر 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) (موسى، 2022، ص189-ص190؛ سويلم، 2024، ص422)، على أن يتم ربط البيانات التي تمت معالجتها بمحتوى مناف للآداب العامة، أو إظهارها بصورة تمس شرف المجني عليه، واعتباره وفقاً للتشريع المصري، أو اتجاه إرادته إلى الإضرار به وفقاً 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 (إبراهيم، 2022، ص202؛ ستين، 2023، ص201).

الخاتمة (النتائج والتوصيات)

إنّ ظاهرة التزييف العميق (Deep fake) من الظواهر المستحدثة، فقد تسارع انتشارها خلال المدى المنظور، وتشكل أحد جوانب تقنية الذكاء الاصطناعي التي أصبحت تهيمن على قطاعات كثيرة، وكغيرها من التقنيات الحديثة التي يمكن أن تُقدم للبشرية الكثير من الفوائد، فهي سلاح ذو حدين، تحمل في طياتها الكثير من المخاطر، وقد تصبح أداة جريمة خطيرة متوفرة وسهلة الوصول والتكلفة في يد المجرمين مسببة الأضرار الجسيمة للأفراد والمؤسسات وحتى زعزعة الأمن الوطني للدول.

قد انتهينا في الختام إلى جملة من نتائج البحث وتوصياته كما يلي:

أولاً: نتائج البحث

1. التشريعات الجنائية العربية، ومنها الأردني جاءت غير كافية لتقديم ما يلزم من نصوص قانونية خاصة قادرة على معالجة مختلف جوانب الاستخدام لتقنية التزييف العميق، كما أنها لم تشر في نصوصها إلى الجهات الأخرى ذات العلاقة بجرائم التزييف العميق، ولم تعالج دور شركات إنتاج تلك التقنيات، ولا سبل الحد من الجرائم المترتبة عليها، ولم تتطرق لدور مزودي هذه الخدمة، إضافة إلى غياب التفصيل الدقيق لجرائم التزييف العميق وإجراءات الوقاية منها أو علاجها، وذلك كما فعل المشرع الصيني والأوروبي بالنص صراحةً على تجريم أفعال التزييف العميق.

2. إن المشرعين الصيني والأوروبي، لم يكتفيا بتفعيل القوانين التقليدية أو حتى القوانين السيبرانية المعتادة في مواجهة أنواع جرائم التزييف العميق (Deep fake)، لِيَقِينِهِم بقصورها في إيجاد خطة تشريعية واضحة لمواجهة التقنية التي تستخدم بطريقة سلبية غير مسبوقة، وحسناً فعل كلا المشرعين في تقرير إجراءات وقائية وجزائية تَحُولُ من إنتاج التزييف العميق لأي غرض إجرامي، وذلك بتفعيل أدوار مزودي الخدمة، وإلزام الجهات المنتجة باتخاذ كل الإجراءات اللازمة لكشف أي تزييف، كما أن كُلًّا من القانونين يحقق ردع لتلك الجرائم عن طريق الإشارة إليها، وبيان العقوبات المترتبة على أي استخدامات سلبية لهذه التقنية.

3. 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.

4. 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، وزعزعة الأمن في المجتمع، ومن المخاطر الاقتصادية لتقنية التزييف العميق الاحتيال والتأثير على البورصة والابتزاز المالي، هذا بالإضافة إلى المخاطر الاجتماعية المتمثلة في التشهير، والانتقام الإباحي، ونشر أخبار كاذبة، والابتزاز الجنسي.

ثانياً: توصيات البحث

1. تستلزم المواجهة الجنائية لتقنية التزييف العميق في الدول العربية، ومنها الأردن التدخل التشريعي وتنظيمها تنظيماً واضحاً، سواء تم ذلك عن طريق تشريع خاص وهو الأفضل، أو تعديل النصوص الموجودة بما يلائم التقدم التكنولوجي بخصوص تقنية التزييف العميق، لذلك نرى من الأفضل:

- ضرورة وضع تعريف قانوني دقيق لتقنية التزييف العميق في قانون الجرائم الإلكترونية الأردني، بما يحد من الغموض التشريعي، ويحقق مبدأ الشرعية الجزائية.

- ضرورة وضع نص تجريمي مستقل في قانون الجرائم الإلكترونية الأردني، تكون صيغته على النحو الآتي: " مع مراعاة أي عقوبة أشد منصوص عليها في أي قانون آخر، يُعاقب كل من استخدم تقنية التزييف العميق بقصد ارتكاب أي من الجرائم المنصوص عليها في هذا القانون أو أي جريمة معاقب عليها بموجب أي تشريع آخر، بالحبس من ستة أشهر إلى ثلاث سنوات، وبغرامة لا تقل عن 2000 دينار، ولا تزيد على 5000 دينار، أو بكلتا هاتين العقوبتين".

2. ضرورة إلزام شركات الإنتاج والتشغيل المحلية المنتجة لهذه التقنية، وإلزام مزودي الخدمة بإجراءات منع الاستخدام المسيء، وأن عليهم أن يتحققوا من بيانات المستخدم وهويته، وتشكيل وحدات مرافقة خاصة، مُكَلَّفَة بإزالة ما يجدونه من محتوى مزيف، وإبلاغ السلطات عن عمليات التزييف العميق.

3. ضرورة 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.

4. نهيب بجهاز الأمن العام إنشاء وحدات متخصصة بهذه التقنية، لتتعامل بسرعة وكفاءة عالية مع ما يردهم من شكاوى في مجالات التزييف العميق.

المصادروالمراجع

إبراهيم، م. (2022). *المسؤولية الجنائية عن جرائم الروبوت: دراسة تحليلية* (ط1). دار النهضة العربية.

أبو يوسف، م. (2025). التنظيم القانوني للتزييف العميق في قانون الذكاء الاصطناعي الصادر عن الاتحاد الأوروبي. *مجلة العلوم القانونية والاقتصادية*، 67(1).

أبو العلا، أ. (2024). المواجهة الجنائية لتقنية الديب فيك (Deep fake). *مجلة العلوم القانونية والاقتصادية*، 66(3).

أبو الوفا، م. (2025). التزييف العميق الإلكتروني والذكي وانتهاك البيانات والمعلومات الشخصية للغير: دراسة تحليلية تأصيلية مقارنة بين القانونين الإماراتي والمصري. *مجلة الأمن والقانون*، 33(2).

أحمد، ع. (2021). *شرح قانون العقوبات: القسم العام* (ط4). دار الثقافة للنشر والتوزيع.

البيومي، ر. (2023). الحماية القانونية من مخاطر تطبيقات التزييف العميق في الفقه الإسلامي والقانون الوضعي: دراسة تحليلية مقارنة. *مجلة روح القوانين* (عدد خاص، المؤتمر الدولي الثامن – التكنولوجيا والقانون).

حسني، م. (2024). *شرح قانون العقوبات: القسم العام: النظرية العامة للجريمة والنظرية العامة للعقوبة والتدبير الاحترازي* (ط12). دار النهضة العربية.

الحكيم، ر. (2025). الجوانب القانونية للتزييف العميق. *مجلة البحوث الفقهية والقانونية* (48).

زكير، أ. (2022). جريمة التزييف الإباحي العميق: دراسة مقارنة. *مجلة القانون*، 11(7).

ستين، ع. س. (2023). *جرائم التشهير والابتزاز الإلكتروني عبر وسائل السوشيال ميديا*. دار الأهرام للنشر والتوزيع والإصدارات القانونية.

سرور، أ. (2023). *الوسيط في قانون العقوبات: القسم العام* (ط10). دار النهضة العربية.

سويلم، م. (2024). *شرح قانون جرائم تقنية المعلومات* (ط1). دار المطبوعات الجامعية.

الشريف، م. (2022). جريمة الانتقام الإباحي عبر تقنية التزييف العميق (Deep fake) والمسؤولية الجنائية عنها. *مجلة الحقوق للبحوث القانونية والاقتصادية*، (1).

العبيدي، ع. (2022). *التطبيقات المعاصرة للجرائم الناتجة عن الذكاء الاصطناعي* (ط1). المركز العربي للنشر والتوزيع.

القاضي، ر. (2020). *شرح قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018 مقارناً بالتشريعات المقارنة والمواثيق الدولية* (ط1). مركز الدراسات العربية.

اللمعي، ي. (2025). المكافحة الجنائية لظاهرة التزييف العميق باستخدام أنظمة الذكاء الاصطناعي في ضوء السياسة التشريعية المعاصرة: دراسة مقارنة

تحليلية. *المجلة القانونية والقضائية*، 19(1).
المجالي، ن. (2023). *شرح قانون العقوبات: القسم العام: دراسة تحليلية في النظرية العامة للجريمة والمسؤولية الجزائية* (ط8). دار الثقافة للنشر والتوزيع.
محرم، أ. (2022). استخدامات الذكاء الاصطناعي (AI): استخدام تقنية التزييف العميق (Deep fake) في قذف الغير أنموذجاً: دراسة فقهية مقارنة معاصرة. *مجلة البحوث الفقهية والقانونية*، 34(39).
مغايرة، ع. د. (2024). جرائم الذكاء الاصطناعي وسبل مواجهتها: جرائم التزييف العميق أنموذجاً. *المجلة الدولية للقانون*، 13(2).
موسى، ح. (2022). *الجرائم المرتكبة عبر وسائل التواصل الاجتماعي* (ط2). دار النهضة العربية.
نايل، إ. (2020). *قانون العقوبات: القسم العام (النظرية العامة للجريمة)* (ط2). دار النهضة العربية.
النجار، س. (2024). المواجهة الجنائية للجرائم الناشئة عن استخدام تقنية التزييف العميق. *مجلة العلوم القانونية*، 39(2).

REFERENCES

Abu al-‘Ula, A. (2024). Al-muwājahah al-jinā’īyah li tiqaniyat al-deepfake. *Majallat al-‘Ulūm al-Qānūnīyah wal-Iqtiṣādīyah, 66*(3).

Abu al-Wafa, M. (2025). Tazyīf al-‘amīq al-ilktrūnī wal-dhakī wa-intihāk al-bayānāt wal-ma‘lūmāt al-shakhṣīyah lil-ghayr: Dirāsah ta’ṣīlīyah muqāranah bayn al-qānūnayn al-imārātī wal-miṣrī. *Majallat al-Amn wal-Qānūn, 33*(2).

Abu Yosef, M. (2025). Al-tanẓīm al-qānūnī lil-tazyīf al-‘amīq fī qānūn al-dhakā’ al-iṣṭinā‘ī al-ṣādir ‘an al-ittiḥād al-ūrūbī. *Majallat al-‘Ulūm al-Qānūnīyah wal-Iqtiṣādīyah, 67*(1).

Ahmad, A. (2021). *Sharḥ Qānūn al-‘uqūbāt: Al-qism al-‘āmm* (4th ed.). Dār al-Thaqāfah lil-Nashr wal-Tawzī‘.

Al-‘Ubīdī, O. (2022). *Al-taṭbīqāt al-mu‘āṣirah lil-jarā’im al-nātijah ‘an al-dhakā’ al-iṣṭinā‘ī* (1st ed.). Al-Markiz al-‘Arabi lil-Nashr wal-Tawzī‘.

Al-Bayoumi, R. (2023). Al-ḥimāyah al-qānūnīyah min makhāṭir taṭbīqāt al-tazyīf al-‘amīq fī al-fiqh al-Islāmī wal-qānūn al-waḍ‘ī: Dirāsah taḥlīlīyah muqāranah. *Majallat Rūḥ al-Qānūn* (Special issue, The 8th International Conference: Technology and Law).

Al-Hakim, R. (2025). Al-jawānib al-qānūnīyah lil-tazyīf al-‘amīq. *Majallat al-Buḥūth al-Fiqhiyah wal-Qānūnayah, 48*.

Al-Lam’i, Y. (2025). Al-mukāfaḥah al-jinā’īyah li ẓāhirat al-tazyīf al-‘amīq bi istikhdām anẓimat al-dhakā’ al-iṣṭinā‘ī fī ḍū’ al-siyāsah al-tashrī‘īyah al-mu‘āṣirah: Dirāsah muqāranah taḥlīlīyah. *Legal Magazine, 19*(1).

Al-Majali, N. (2023). *Sharḥ Qānūn al-‘uqūbāt: Al-qism al-‘āmm: Dirāsah taḥlīlīyah fī al-naẓarīyah al-‘āmm lil-jarīmah wal-mas’ūlīyah al-jazā’īyah* (8th ed.). Dār al-Thaqāfah lil-Nashr wal-Tawzī‘.

Al-Najjar, S. (2024). Al-muwājahah al-jinā’īyah lil-jarā’im al-nāshi’ah ‘an istikhdām tiqaniyat al-tazyīf al-‘amīq. *Majallat al-‘Ulūm al-Qānūnayah, 39*(2).

Al-Qadi, R. (2020). *Sharḥ Qānūn mukāfaḥat jarā’im tiqaniyat al-ma‘lūmāt raqam 175 li sanat 2018 muqāranan bil-tashrī‘āt al-muqāranah wal-mawāthīq al-duwalīyah* (1st ed.). Markiz ad-Dirāsāt al-‘Arabiyah.

Al-Sharif, M. (2022). Jarīmat al-intiqām al-ibāḥī ‘abra tiqaniyat al-tazyīf al-‘amīq wal-mas’ūlīyah al-jinā’īyah ‘anhā. *Majallat al-Ḥuqūq lil-Buḥūth al-Qānūnayah wal-Iqtiṣādiyah* (1).

Broinowski, A., & Martin, F. (2024). Beyond the deepfake problem: Benefits, risks and regulation of generative AI screen technologies. *Media International Australia*. https://doi.org/10.1177/1329878X241288034

Husni, M. (2024). *Sharḥ Qānūn al-‘uqūbāt: Al-qism al-‘āmm: Al-naẓarīyah al-‘āmm lil-jarīmah wal-naẓarīyah al-‘āmm lil-‘uqūbah wal-tadbīr al-iḥtirāzī* (12th ed.). Dār al-Nahḍah al-‘Arabiyah.

Ibrahim, M. (2022). *Al-mas’ūlīyah al-jinā’īyah ‘an jarā’im al-rūbūt: Dirāsah taḥlīlīyah* (1st ed.). Dār al-Nahḍah al-‘Arabiyah.

Loovens, J., & Tinmaz, H. (2025). A systematic literature review of deepfakes in forensic science. *Forensic Imaging, 43*, Article 200647. https://doi.org/10.1016/j.fri.2025.200647

Maghayreh, A. (2024). Jarā’im al-dhakā’ al-iṣṭinā‘ī wa-subul muwājahatuhā: Jarā’im al-tazyīf al-‘amīq unmūdhajan. *Al-Majallah al-Duwaliyah lil-Qānūn, 13*(2).

Maharram, A. (2022). Istikhdāmāt al-dhakā’ al-iṣṭinā‘ī (AI): Istikhdām tiqaniyat al-tazyīf al-‘amīq (deepfake) fī qathf al-ghayr: Dirāsah fiqhīyah muqāranah mu‘āṣirah. *Majallat al-Buḥūth al-Fiqhiyah wal-Qānūnayah, 34*(39).

Musa, H. (2022). *Al-jarā'im al-murtakabah 'abra wasā'il al-tawāṣul al-ijtimā'ī* (2nd ed.). Dār al-Nahḍah al-'Arabiyah.

Nayil, I. (2020). *Sharḥ Qānūn al-'uqūbāt: Al-qism al-'āmm (al-naẓarīyah al-'āmm lil-jarīmah)* (2nd ed.). Dār al-Nahḍah al-'Arabiyah.

Sandoval, M. P., de Almeida Vau, M., Solaas, J., et al. (2024). Threat of deepfakes to the criminal justice system: A systematic review. *Crime Science*, *13*, 41. https://doi.org/10.1186/s40163-024-00239-1

Sittin, A. (2023). *Jarā'im al-tashhīr wal-ibtizāz al-iliktrūnī 'abra wasā'il al-sūshiyāl mīdiyā*. Dār al-Haram lil-Nashr wal-Tawzī' wal-Iṣdārāt al-Qānūnīyah.

Surūr, A. (2023). *Al-wasīṭ fī Qānūn al-'uqūbāt: Al-qism al-'āmm* (10th ed.). Dār al-Nahḍah al-'Arabiyah.

Sweilim, M. (2024). *Sharḥ Qānūn jarā'im tiqaniyat al-ma'lūmāt* (1st ed.). Dār al-Maṭbū'āt al-Jāmi'yah.