المسؤولية الجنائية لجريمة التزييف العميق

م.م مها حاتم حسن السعبري

كلية الحقوق/ جامعة النهرين

ma0191027@gmail.com

المستخلص

يمثل التزييف العميق تحولاً نوعياً في ممارسة الجريمة، إذ يتيح إنتاج محتوى مرئي أو سمعي يحاكي الواقع بدرجة عالية من الدقة تفوق وسائل التزوير التقليدية، مستنداً إلى تقنيات الذكاء الاصطناعي والتعلم العميق، وقد أدى انتشار هذه التقنية إلى ظهور مخاطر قانونية متزايدة تمس الثقة في الأدلة الرقمية، وتهدد السمعة والخصوصية والأمن العام، فضلاً عن إمكانية استغلالها في جرائم الاحتيال والتشهير وانتحال الشخصية والتلاعب بالمعلومات، وعلى الرغم من غياب نص صريح يجرم التزييف العميق في القانون العراقي، فإن القضاء والفقه يميلان إلى تكييفه ضمن جرائم التشهير والتزوير والاحتيال المنصوص عليها في قانون العقوبات رقم (111) لسنة 1969، في حين توفر تشريعات مقارنة، كالمصرية والإماراتية والفرنسية والأوروبية، نماذج أكثر تخصصاً في التعامل مع هذه الظاهرة، وإن اختلفت في طبيعتها بين أحكام جنائية مباشرة ومتطلبات تنظيمية تفرض الشفافية والإفصاح عن المحتوى الاصطناعي.

الكلمات المفتاحية: التزييف العميق، المسؤولية الجنائية، الذكاء الاصطناعي، جرائم المعلوماتية.

Abstract

Deepfake technology represents a qualitative shift in the commission of crime, as it enables the creation of visual or audio content that closely mimics reality with a level of accuracy surpassing traditional methods of forgery. Based on artificial intelligence and deep learning technologies, its widespread use has given rise to increasing legal risks that undermine trust in digital evidence and threaten reputation, privacy, and public security. Furthermore, it can be exploited in crimes such as fraud, defamation, identity theft, and information manipulation. Despite the absence of an explicit provision criminalizing deepfakes under Iraqi law, judicial practice and legal scholarship tend to classify such conduct within the offenses of defamation, forgery, and fraud stipulated in Iraqi Penal Code No. 111 of 1969. In contrast, comparative legal systems, including those of Egypt, the United Arab Emirates, France, and the European Union, provide more specialized models for addressing this phenomenon, although they differ in nature, ranging from direct criminal provisions to regulatory requirements mandating transparency and disclosure of AI-generated content.

Keywords: Deepfake; Criminal Liability; Artificial Intelligence; Cybercrime.

المقدمة

شهد العالم في العقد الأخير طفرة غير مسبوقة في تطبيقات الذكاء الاصطناعي، ومن أبرزها تقنية التزييف العميق التي تمكن من إنشاء أو تعديل محتوى صوتي ومرئي يبدو حقيقياً إلى حد يصعب معه على المتلقي العادي تمييزه عن الواقع، وقد ظهرت هذه التقنية لأول مرة بشكل واسع في عام 2017 عبر منصات التواصل الاجتماعي، ثم تطورت بسرعة بفضل خوارزميات التعلم العميق وشبكات التوليد التنافسي (GANs)، حتى أصبح إنتاج الفيديو المزيف ممكناً عبر تطبيقات بسيطة على الهواتف الذكية، ويرتبط هذا التطور التقني بأزمة قانونية عميقة، إذ إن القوانين الجنائية التقليدية وُضعت في سياقٍ مادي يقوم على وثائق ورقية ووسائل تزوير يدوية، بينما يعمل التزييف العميق في فضاء افتراضي غير ملموس، ويستهدف في كثير من الأحيان سمعة الأفراد والمؤسسات. إذ لم يعد تأثير التزييف العميق يقع على الأفراد فحسب، بل يمتد ليشمل الدول والمؤسسات الإعلامية والشركات، فكل هذه الجهات عرضة لحملات تضليل منسقة تستخدم مقاطع مزيفة لقادة سياسيين أو مسؤولين أو صحفيين، ما يُهدد الأمن الوطني والعلاقات الخارجية، وهذا البعد يفرض اعتبار الجريمة جريمةً معلوماتية قد تصل في خطورتها إلى جرائم المساس بالأمن، لا جريمة تشهير فردية فحسب. وعلى الرغم من كل هذه المخاطر التي تولدها تقنية التزييف العميق لاتزال بعض الدول تهمل هذه الخطورة ولم تشرع لها النصوص القانونية ولم تفرد لها عقوبات مخصصة، مما يولد مشكلة في كيفية معالجة هذه الجريمة من حيث هل يمكن اعتبارها كجريمة قائمة بذاتها او صوره مستحدثة من الجرائم التقليدية جرائم الاحتيال والتشهير وهذا ما يدفع بالأوساط القانونية نحو البحث عن تكيف قانوني مناسب لمواجهة هذه التقنية وسد الفراغ التشريعي الى حين تشريع نصوص تعالجها.

أهمية البحث

تكمن أهمية البحث في تناوله لجريمة التزييف العميق بوصفها من الجرائم المستحدثة الناتجة عن التطور المتسارع لتقنيات الذكاء الاصطناعي، لما تثيره من مخاطر تمس السمعة والخصوصية والأمن المعلوماتي. كما تبرز أهميته في بيان مدى كفاية القواعد الجنائية القائمة لمواجهة هذه الجريمة في ظل غياب تنظيم تشريعي خاص بها في العراق، والكشف عن الحاجة إلى تطوير السياسة الجنائية بما يواكب التطورات التقنية الحديثة.

أهداف البحث

يهدف هذا البحث إلى تحقيق الأهداف الآتية:

1. بيان المفهوم القانوني للتزييف العميق وخصائصه التقنية التي تميزه عن التزوير التقليدي.
2. تحليل الأساس القانوني للمسؤولية الجنائية عن التزييف العميق في التشريع العراقي مقارنةً بتشريعات دولية وعربية.
3. تحديد أركان المسؤولية الجنائية المادية والمعنوية في جرائم التزييف العميق.
4. تشخيص الإشكالات الإثباتية والتشريعية التي تعيق مواجهة الجريمة، واقتراح آليات قانونية وتقنية لمواجهة التزييف العميق في السياق العراقي.

مشكلة البحث

تتمحور مشكلة البحث حول تساؤل رئيس مفاده: إلى أي مدى يمكن القول إن التشريعات الجنائية—وعلى رأسها القانون العراقي—توفر إطاراً كافياً لتحمل المسؤولية الجنائية عن جريمة التزييف العميق، من حيث التكييف القانوني، وأركان الجريمة، ووسائل الإثبات؟ وانبثاقاً عن ذلك، تظهر تساؤلات فرعية تتعلق بطبيعة الفعل الجنائي في التزييف العميق، وعلاقته بجرائم التزوير والاحتيال والتشهير، ومدى قدرة الأدلة الرقمية على كشف المحتوى المزيف.

منهج البحث

اعتمد البحث المنهج التحليلي في دراسة النصوص القانونية وأركان المسؤولية الجنائية، والمنهج الوصفي في عرض الظاهرة التقنية وخصائصها، والمنهج المقارن في استعراض التشريعات العراقية والمصرية والإماراتية والفرنسية والأوروبية، بغية إبراز أوجه الاتفاق والاختلاف والتكامل بينها فيما يخص معالجة هذه الظاهرة التقنية التي تحمل أوجه ومعالم اجرامية.

هيكلية البحث

تم تقسيم هذا البحث إلى مقدمة وثلاثة مباحث وخاتمة على النحو الآتي:

- المبحث الأول: الإطار المفاهيمي والقانوني لجريمة التزييف العميق.
- المبحث الثاني: الأساس القانوني للمسؤولية الجنائية عن التزييف العميق.
- المبحث الثالث: التحديات القانونية وسبل المواجهة.

المبحث الأول

الإطار المفاهيمي والقانوني لجريمة التزييف العميق

يُعد التزييف العميق من أبرز التطبيقات الحديثة للذكاء الاصـــطناعي التي أثارت تحديات قانونية غير مســـبوقة، نتيجة قدرته على إنتاج محتوى رقمي مزيف يصعب تمييزه عن المحتوى الحقيقي، وقد أدى انتشار هذه التقنية إلى ظهور أنماط جديدة من السلوك الإجرامي تمس الحقوق الشخصية والمصالح العامة، الأمر الذي يقتضي بيان مفهوم التزييف العميق وخصائصه، فضلاً عن استعراض التطور التقني الذي أسهم في ظهوره وانتشاره، وذلك وفق الآتي:

المطلب الأول

ماهية التزييف العميق وخصائصه

إن تحديد ماهية التزييف العميق يمثل الخطوة الأولى لفهم الأبعاد القانونية المترتبة عليه، إذ يتطلب الأمر الوقوف على مفهومه وتمييزه عن الصـــور التقليدية للتزوير، فضـــلاً عن بيان الخصـــائص التقنية التي تمنحه القدرة على محاكاة الواقع بدرجة عالية من الدقة، وهو ما يبرر خصوصية المعالجة القانونية لهذه الظاهرة.

أولاً: تعريف التزييف العميق وتمييزه عن التزوير التقليدي

يُعرَف التزييف العميق، بأنه شكل من أشكال المحتوى السمعي البصري المُنشأ أو المُتلاعب به باستخدام الذكاء الاصطناعي، يصور شخصاً أو شيئاً بشكل خاطئ، بحيث يبدو للمشاهد العادي حقيقياً[1]. ويتكون المصطلح من كلمتي (عميق) إشارةً إلى التعلم العميق، و(مزيف) إشارةً إلى عدم مطابقة المحتوى للواقع[2].

ويميز الفقه المعاصر بين التزييف العميق والتزوير التقليدي على عدة محاور: فالتزوير التقليدي—كما عرفه قانون العقوبات العراقي—هو تغيير الحقيقة بقصد الغش في سند أو وثيقة أو أي محرر آخر[3]، ويستلزم عادةً محرراً مادياً أو إلكترونياً يحمل دلالة ثبوتية، أما التزييف العميق فيستهدف الحقيقة المرئية أو السمعية ذاتها لا المحرر فقط، ولا يتطلب بالضرورة إنشاء وثيقة، بل يكفي إنتاج مقطع فيديو أو تسجيل صوتي يُظهر شخصاً وهو يقول أو يفعل ما لم يفعله[4].

كما يختلف التزوير التقليدي في كونه يترك—في الغالب—آثاراً فنية يمكن للخبير اكتشافها، بينما يصل التزييف العميق في أحدث صوره إلى مستوى يصعب معه التمييز دون أدوات تحليل تقنية متخصصة[5]. ومن ثم، فإن التكييف القانوني للتزييف العميق تحت جريمة التزوير التقليدية يبقى ممكناً في بعض الصور—حين يُعدل محتوى ذا صفة ثبوتية—لكنه لا يغطي جميع أشكال الإساءة، كالتشهير بمقطع فيديو مزيف لا يُعد محرراً في المعنى التقليدي.

ويمكن إضافة تمييز ثالث يتعلق بالغاية فالتزوير التقليدي يهدف غالباً إلى إحداث اعتقاد قانوني أو مالي بحقيقة وهمية (تزوير عقد، شهادة، عملة). أما التزييف العميق فيستهدف—في أغلب حالاته الإجرامية—إحداث اعتقاد اجتماعي أو إعلامي بوقائع لم تقع (أن فلاناً قال كذا، أو تصرف كذا)، وهذا الفارق مهم في التكييف، لأن جرائم التزوير ترتبط بالغش في المحرر، بينما جرائم التزييف العميق ترتبط بالغش في التصور[6].

ثانياً: الخصائص التقنية والقانونية المميزة له

تتميز تقنية التزييف العميق بمجموعة من الخصائص التقنية من أبرزها: الاعتماد على التعلم العميق والشبكات التنافسية GANs التي تتنافس فيما بينها لإنتاج محتوى أكثر واقعية[7]، وإمكانية استنساخ الوجه والصوت معاً، وانخفاض كلفة الإنتاج واتساع نطاق الانتشار عبر الإنترنت، وصعوبة اكتشاف التزييف بالوسائل العادية.

---

(1) سحر فؤاد مجيد النجار، المواجهة الجنائية للجرائم الناشئة عن استخدام تقنية التزييف العميق، مجلة العلوم القانونية، المجلد 39، العدد الثاني، 2024، ص 580.

(2) علاء الدين منصور مغايرة، جرائم الذكاء الاصطناعي وسبل مواجهتها: جرائم التزييف العميق نموذجًا، المجلة الدولية للقانون، جامعة قطر، المجلد 13، العدد 2، 2024، ص 131.

(3) المادة (286) من قانون العقوبات العراقي رقم (111) لسنة 1969 المعدل.

(4) صابرين جاسم مكطوف، أميل جبار عاشور، الأحكام الموضوعية لجريمة التزييف العميق ومعالجتها القانونية (دراسة مقارنة) ، مجلة آشور للعلوم القانونية والسياسية، المجلد 2، العدد 2، 2025، ص 85.

(5) رباب مصطفى عبد المنعم الحكيم، الجوانب القانونية للتزييف العميق، مجلة الحقوق، جامعة الأزهر، العدد 48، 2025، ص 2679.

(6) صابرين جاسم مكطوف، أميل جبار عاشور، مرجع سابق، ص 85.

(7) سحر فؤاد مجيد النجار، مرجع سابق، ص 581.

أما الخصائص القانونية المميزة لها فتتمثل في:

1. طبيعة الفعل الافتراضية التي لا تترك أثراً مادياً مباشراً.
2. تعددية الضحايا والأطراف (الشخص المستهدف، ومنشئ المحتوى الأصلي، وناشر المقطع، ومنصة الاستضافة).
3. الطبيعة العابرة للحدود، إذ يمكن ارتكاب الجريمة من خارج إقليم الضحية.
4. خطر المساس بالثقة في الأدلة الرقمية، بما في ذلك استخدام التزييف في الإثبات الجنائي أو التلاعب بالتحقيقات[1].
5. ازدواجية الاستخدام بين أغراض مشروعة (السينما، التعليم، الترفيه) وأخرى إجرامية، مما يفرض تمييزاً بين التزييف المشروع وغير المشروع في التشريع[2].

المطلب الثاني

التطور التقني لجريمة التزييف العميق

لم يظهر التزييف العميق بصورة مفاجئة، بل كان نتيجة تطور متسارع في تقنيات الذكاء الاصطناعي والتعلم العميق ومعالجة البيانات الرقمية، ولأهمية الخلفية التقنية في فهم طبيعة هذه الجريمة، يقتضي البحث تتبع نشأة هذه التقنيات وتطورها، ثم بيان أبرز الصور والأشكال التي يتجسد من خلالها التزييف العميق في الواقع العملي.

أولاً: نشأة وتطور تقنيات الذكاء الاصطناعي المستخدمة في التزييف

بدأ التزييف العميق كتقنية فرعية من الذكاء الاصطناعي والتعلم الآلي، حين طور الباحث (إيان غودفيلو) شبكات التوليد التنافسي عام 2014، مما مكن الحواسيب من إنتاج صور وصوت واقعيين انطلاقاً من بيانات تدريبية[3]. وفي 2017 ظهرت أول تطبيقات التزييف العميق على منصة (Reddit)، ثم تسارع التطور حتى أصبح إنتاج فيديو مزيف ممكناً عبر تطبيقات مثل (Reface وFaceApp) تنصب على منصات عديدة مثل (الايفون) و (الاندرويد)[4].

---

(1) اياد عبد حمزة بعيوي، الإطار القانوني لمكافحة جرائم التزييف العميق وأثره على الإثبات الجنائي، مجلة آشور للعلوم القانونية والسياسية، المجلد 3، العدد 1، 2026، ص 342.

(2) رضا ابراهيم عبدالله البيومي، الحماية القانونية من مخاطر التزييف العميق في الفقه الاسلامي والقانون الوضعي، مجلة روح القانون، جامعة طنطا، المجلد 35، العدد 102، 2023، ص828.

(3) I. J. Goodfellow et al., Generative Adversarial Nets, Proceedings of the 28th Annual Conference on Neural Information Processing Systems (NeurIPS), 2014, p. 1.

(4) Shivangi, A, 15 Best Deepfake Apps & Websites that You Must Try (2023). https://www.smartprix.com/bytes/14-best-deepfake-apps-websites-for-entertainment

وقد أدى هذا التطور إلى انتقال الجريمة من نطاق المحترفين التقنيين إلى نطاق المستخدم العادي، ما وسع دائرة الجناة المحتملين وعقد تحديد المسؤولية الجنائية[1]. وعلى هذا اصبح عدد الفيديوهات المزيفة يتضاعف بوتيرة متسارعة، وأن النسبة الأكبر منها يُستخدم في محتوى إباحي انتقامي ضد النساء تحديداً[2].

ثانياً: صور وأشكال التزييف العميق (الصوت، الصورة، الفيديو)

تتعدد صور التزييف العميق بحسب الوسيط المستخدم:

1. **تزييف الصورة**: يتم عبر تركيب وجه شخص على جسد آخر أو تعديل تعابير الوجه، ويُستخدم غالباً في الابتزاز والتشهير.
2. **تزييف الصوت**: يعتمد على استنساخ صوت الشخص وإنتاج كلام لم ينطق به، وقد استُخدم في عمليات احتيال مالية جسيمة، ومن الأمثلة لهذه العمليات هي عملية الاحتيال الصوتي الشهرية التي وقعت على مدير تنفيذي في شركة بريطانية بمبلغ 243,000 دولار في عام 2019[3].
3. **تزييف الفيديو**: وهو الأخطر والأكثر انتشاراً، إذ يجمع بين الصورة والصوت ويُستخدم في التشهير السياسي، والحملات الانتخابية، والدعاية المضللة، والإباحية الانتقامية[4].

وتُضيف الدراسات الإعلامية بعداً اجتماعياً خطيراً، إذ أظهرت أبحاث في مجال التزييف العميق أن المحتوى المزيف يُستخدم في التلاعب بالرأي العام، وصناعة أزمات سياسية، واستهداف النساء بصورة غير متناسبة مع غيرهن من الفئات[5].

وفي السياق العراقي، يكتسب هذا البعد أهمية خاصة في ظل حساسية المشهد السياسي والاعتماد المتزايد على المنصات الرقمية كمصدر للأخبار، ما يجعل غياب التشريع المتخصص ثغرة أمنية لا يمكن تجاهلها.

ومن الجدير بالذكر أن التزييف العميق لا يُمارس دائماً بقصد إجرامي صرف، إذ توجد استخدامات مشروعة في صناعة السينما والتعليم، وإعادة تمثيل الشخصيات التاريخية، والسخرية الواضحة. ومن ثم، فإن أي تشريع جنائي يجب أن يفرق بين التزييف المشروع—الذي يُفصح عن طبيعته الاصطناعية—والتزييف الخبيث الذي يستهدف الإضرار أو التضليل[6]. وهذا التمييز يعكس توازناً بين حرية التعبير والإبداع من جهة، وحماية السمعة والخصوصية من جهة أخرى.

المبحث الثاني

---

(1) سحر فؤاد مجيد النجار، مرجع سابق، ص 585.

(2) علاء الدين منصور مغايرة، مرجع سابق، ص 136.

(3) J. Damiani, "A Voice Deepfake Was Used to Scam a CEO Out of $243,000", Forbes, 2019, available at: https://www.forbes.com/sites/jessedamiani/2019/09/03/a-voice-deepfake-was-used-to-scam-a-ceo-out-of-243000/

(4) سحر فؤاد مجيد النجار، مرجع سابق، ص 589.

(5) B. Chesney & D. Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security", California Law Review, Vol. 107, 2019, pp. 1753.

(6) علاء الدين منصور مغايرة، مرجع سابق، ص 135.

الأساس القانوني للمسؤولية الجنائية عن التزييف العميق

يُعد تحديد الأساس القانوني للمسؤولية الجنائية عن جريمة التزييف العميق من المسائل الدقيقة في نطاق القانون الجنائي المعاصر، وذلك لارتباط هذه الجريمة بالتطورات التقنية الحديثة التي لم تكن مألوفة عند وضع التشريعات التقليدية، ويثير هذا النوع من الجرائم إشكالات تتعلق بكيفية تكييفه قانونياً، وما إذا كان يندرج ضمن الجرائم المعلوماتية أو يمكن مقارنته بجرائم التزوير والاحتيال التقليدية، الأمر الذي يستدعي بحث طبيعته القانونية بدقة. وانطلاقاً من ذلك، يقتضي البحث بيان التكييف القانوني لجريمة التزييف العميق في ضوء التشريع المقارن، ثم تحليل أركان المسؤولية الجنائية المترتبة عليها، من حيث الركن المادي والركن المعنوي، باعتبارهما الأساس الذي تقوم عليه المسؤولية الجنائية في هذا النوع من الجرائم المستحدثة. وذلك على وفق الآتي:

المطلب الأول

التكييف القانوني لجريمة التزييف العميق

تُثير جريمة التزييف العميق جدلاً فقهياً وقانونياً بشأن طبيعتها القانونية، نظراً لعدم وجود نصوص صريحة في أغلب التشريعات تنظمها بشكل مباشر، بما في ذلك التشريع العراقي، لذلك يتم البحث في إمكانية إدراجها ضمن جرائم المعلوماتية، أو قياسها على جرائم التزوير والاحتيال، وفقاً لمدى تحقق عناصر التشابه بينهما، وهو ما يحدد الإطار القانوني الذي تخضع له هذه الجريمة وآثارها الجزائية.

أولاً: إدراجها ضمن جرائم المعلوماتية

يمثل إدراج التزييف العميق ضمن جرائم المعلوماتية التوجه التشريعي الأنسب، لأن الفعل يُرتكب بوساطة تقنية المعلومات والشبكات، ويستهدف البيانات والمحتوى الرقمي، وقد سارعت عدة دول عربية في هذا الاتجاه، منها مصر التي أصدرت قانون مكافحة جرائم تقنية المعلومات رقم (175) لسنة 2018، والإمارات التي أصدرت المرسوم بقانون اتحادي رقم (34) لسنة 2021 بشأن مكافحة الشائعات والجرائم الإلكترونية[1].

أما العراق، فيواجه فراغاً تشريعياً ملحوظاً، إذ لم يُنشر بعد قانون متخصص للجرائم المعلوماتية رغم طرح مشاريع متعددة منذ 2011[2]. وفي هذا الفراغ، يضطر القضاء إلى تكييف السلوكيات الرقمية ضمن قانون العقوبات العام، وهو ما يثير إشكالات في التطبيق لاختلاف البنية التقنية للجريمة عن الفعل التقليدي[3].

إن القضاء العراقي استخدم مواد متفرقة من قانون العقوبات—منها المواد المتعلقة بالتهديد والتشهير والاحتيال—في ملاحقة قضايا رقمية، لكن دون اتساق تشريعي يوحد التكييف[4]. كما أن مشاريع قانون الجرائم المعلوماتية السابقة التي طرحت في البرلمان العراقي وصفت بأنها تتضمن عبارات فضفاضة قد تُستخدم في تضييق الحريات،

---

(1) رباب مصطفى عبد المنعم الحكيم، مرجع سابق، ص 1.

(2) هشام كاظم، «توسيع الاشتباه بدل التنظيم.. قراءة قانون الجرائم الإلكترونية في العراق»، بحث منشور على الانترنت، 2024، الرابط : https://jummar.media/11958 ، تاريخ اخر زيارة 2026/6/10.

(3) سحر فؤاد مجيد النجار، مرجع سابق، ص 578.

(4) هشام كاظم، مصدر سابق.

ما أدى إلى تعطيل إقرارها، وهذا يفرض على المشرع العراقي صياغة دقيقة تُجريم التزييف العميق دون إطلاق يد السلطة في معاقبة المحتوى المشروع[1].

ومن صور الجرائم التي يُكيَف فيها التزييف العميق في العراق عملياً مثل نشر فيديو مزيف يتضمن سباً أو قذفاً يحال ال (المواد 433–434) من قانون العقوبات، واستخدام فيديو مزيف في عملية نصب يحال الى المادة (456)، ونشر محتوى يمس الأمن الوطني إذا اقترن بتحريض أو تضليل جماهيري (مواد أخرى حسب التكييف)، غير أن كل هذه التكييفات تفتقر إلى معيار موحد، ما يُنتج تفاوتاً في الأحكام ويُضعف الردع العام.

ويرى الفقه القانوني المعاصر أن جريمة التزييف العميق جريمة معلوماتية مستقلة في مضمونها، لأنها لا تقتصر على تعديل محرر بل على توليد محتوى رقمي يُغير تصور الواقع، ومن ثم يستلزم تعريفاً قانونياً صريحاً خاص بها يحتوي على وصف كامل لها يتضمن الإشارة الى طبيتها وهي إنشاء أو تعديل محتوى صوتي أو مرئي باستخدام الذكاء الاصطناعي، ونسبة المحتوى إلى شخص دون موافقته، النشر أو الترويج، ويتضمن الغاية منها وهي قصد الإضرار أو التضليل، والعقوبة المخصصة لها[2].

ثانياً: صلتها بجرائم التزوير والاحتيال

عند غياب نص متخصص، يلجأ القضاء إلى التكييف بالتوسع في الجرائم التقليدية، لتشمل صوراً جديدة تندرج فيها الظواهر المستحدثة التي تفتقر الى معالجة قانونية صريحة، ولعل أبرز تكيف ممكن لظاهرة التزييف العميق في ظل غياب المعالجة القانونية لها، وهي اعتبارها صوره من صور احد الجرائم الآتية:

1. **التزوير**: يمكن تكييف بعض صور التزييف العميق—حين يُستخدم المحتوى المزيف كدليل أو وثيقة في إجراء قانوني—ضمن جريمة التزوير المنصوص عليها في المادة (286) من قانون العقوبات العراقي، غير أن هذا التكييف يظل محدوداً إذا كان الفعل يقتصر على نشر فيديو تشهيري لا يُعد محرراً في المعنى القانوني.
2. **الاحتيال**: تُكيَف صور التزييف المستخدمة للحصول على منفعة مالية—كانتحال شخصية مسؤول أو ترويج عملة رقمية وهمية—ضمن جرائم الاحتيال والنصب المنصوص عليها في المادة (456) من قانون العقوبات العراقي، وتشير الدراسات إلى وقوع حالات احتيال دولية باستخدام مكالمات فيديو مزيفة.
3. **التشهير والسب والقذف**: يُعد التكييف الأكثر شيوعاً في العراق، إذ يُصنف نشر فيديو مزيف يمس السمعة ضمن المواد (433) و(434) من قانون العقوبات المتعلقة بالقذف والسب، غير أن هذا التكييف لا يعاقب إنشاء المحتوى بذاته إذا لم يُنشر، كما أنه لا يعالج حالات التلاعب غير التشهيري.

---

(1) صفاء عياد ، قانون جرائم المعلوماتية في العراق، بحث منشور على الانترنت، 2022، الرابط: https://smex.org/iraqi-cybercrime-draft-law-in-suspension/ ، تاريخ اخر زيارة 2026/6/10

(2) صابرين جاسم مكطوف، أميل جبار عاشور، مرجع سابق، ص 86.

وبالمقارنة، نجد أن القانون الفرنسي في قانون SREN رقم (2024-449) عالج المشكلة صراحةً بتجريم أي نشر لمحتوى مرئي أو سمعي مُولَّد خوارزمياً يمثل صورة أو كلام شخص دون موافقته، في المادة (226-8) من قانون العقوبات[1]، وهو نموذج تكييف مباشر يتجاوز اللجوء إلى جرائم التزوير أو التشهير.

ففي الوقت الذي يمكن تكييف التزييف العميق في قانون العقوبات العراقي رقم (111) لسنة 1969 على انه جريمة من جرائم السب والقذف (المادتان 433 و434)، أو التزوير (المادة 286) إذا اقترن بمحرر، أو الاحتيال عند تحقق منفعة مالية[2]. فأن التشريع المصري يوفر معالجةً وتكييفاً أفضل لهذه الجرائم فقد وضع قانون (175) لسنة 2018 إطاراً للجرائم المعلوماتية، إذ تعاقب المادة (25) منه على نشر معلومات أو صور تمس الخصوصية أو القيم الأسرية سواء كانت المعلومات صحيحة أو خاطئة، بالحبس ستة أشهر على الأقل وغرامة (50,000 – 100,000) جنيه. وتعاقب المادة (26) منه على استخدام برنامج معلوماتي لمعالجة بيانات شخصية وربطها بمحتوى مسيء، بالحبس سنتين على الأقل[3].

وفضلاً عن التشريع المصري فأن التشريع الإماراتي يعالج التزييف العميق من خلال الجمع بين مواد في قانون العقوبات الاتحادي وقانون مكافحة الجرائم الإلكترونية، فتُشدد المادة (44) من المرسوم (34) لسنة 2021 العقوبة عند التشهير بوسائل تقنية، كما تُعاقب المادة (40) الاحتيال الإلكتروني بعقوبات بالغة الصرامة. وقد أطلقت الإمارات دليل التزييف العميق كإطار توعوي وتنظيمي[4].

وفي التشريع الفرنسي يتم يجرم النشر دون موافقة حتى لو لم يقصد الجاني التشهير، ويعاقب بسنة حبس و15,000 يورو، وتُرفع العقوبة إلى سنتين و45,000 يورو عند النشر عبر الإنترنت، واستحدثت المادة (226-8-1) عقوبات خاصة بالمحتوى الإباحي المزيف.

وفي التشريع الأوروبي، يتجه قانون الذكاء الاصطناعي (AI Act) إلى تنظيم استخدام أنظمة الذكاء الاصطناعي عبر فرض التزامات واضحة على مزودي هذه الأنظمة ومستخدميها، لا سيما فيما يتعلق بوجوب الإفصاح عن المحتوى المُنشأ أو المُعدل بواسطة تقنيات الذكاء الاصطناعي. كما يفرض القانون جزاءات مالية ذات طابع إداري قد تصل إلى 35 مليون يورو أو 7% من إجمالي رقم الأعمال العالمي السنوي، أيهما أعلى، في حال ارتكاب مخالفات جسيمة. في المقابل، لا يتضمن هذا التنظيم إنشاء جريمة جنائية موحدة على مستوى الاتحاد الأوروبي،

---

(1) المادة (226-8) من قانون العقوبات الفرنسي. متاح عبر الرابط: https://www.legifrance.gouv.fr/codes/article_lc/LEGIARTI000049571542/2024-05-23

(2) صابرين جاسم مكطوف، أميل جبار عاشور، مرجع سابق، ص 90.

(3) المواد (25) و (26) من قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018.

(4) Baker McKenzie, "United Arab Emirates: Deepfakes and the Use of Artificial Intelligence (AI)", 11 June 2024, available at: https://insightplus.bakermckenzie.com/bm/data-technology/united-arab-emirates-deepfakes-and-the-use-of-artificial-intelligence-ai-legal-issues-and-considerations

وإنما يترك مسألة التجريم وتحديد المسؤولية الجنائية للقوانين الوطنية في الدول الأعضاء، بما يعكس الطبيعة التنظيمية غير الجنائية لهذا الإطار التشريعي[1].

ويتضح من هذا العرض أن العراق يقع في المرتبة الأدنى من حيث التخصص التشريعي في معالجة الجرائم المعلوماتية بشكل عام وجريمة التزييف العميق بشكل خاص، ما يفرض على المشرع العراقي الاستفادة من التجارب المقارنة في معالجة الظواهر الاجرامية الحديثة دون إغفال خصوصية النظام القانوني العراقي.

المطلب الثاني

أركان المسؤولية الجنائية في التزييف العميق

تقوم المسؤولية الجنائية في جريمة التزييف العميق، شأنها شأن باقي الجرائم، على مجموعة من الأركان الأساسية التي لا تقوم الجريمة بدونها، غير أن خصوصية هذه الجريمة التقنية تفرض إعادة قراءة الركن المادي من حيث الوسائل المستخدمة في ارتكابها، والتي تعتمد على تقنيات الذكاء الاصطناعي، فضلاً عن ضرورة توافر الركن المعنوي المتمثل بالقصد الجنائي، سواء كان عاماً أو خاصاً، بحسب طبيعة الفعل المرتكب والغاية منه.

أولاً: الركن المادي (الفعل الإجرامي ووسائل ارتكابه)

يتكون الركن المادي للجريمة من السلوك الإجرامي والنتيجة الجرمية وعلاقة السببية التي تربط بينهما، اما وعلى نفس السياق فأن الركن المادي لجريمة التزييف العميق—في صورتها الجنائية— يتكون من هذه العناصر:

1. **السلوك الاجرامي**: إنشاء أو تعديل محتوى رقمي (صوت، صورة، فيديو) باستخدام خوارزميات الذكاء الاصطناعي، وقد يكون الفعل مكتملاً بمجرد الإنتاج إذا نص القانون على ذلك—كما في التشريع الفرنسي— أو يشترط النشر كما في بعض التكييفات العراقية القائمة على جرائم التشهير.
2. **النتيجة**: المساس بمصلحة محمية قانوناً: السمعة، الخصوصية، المال، الأمن العام، أو نزاهة الإجراءات القضائية[2].
3. **العلاقة السببية**: بين الفعل والنتيجة، وهي في التزييف العميق غالباً واضحة عند النشر، لكنها تتعقد إذا وُجد تدخل وسطاء (منصات، مزودو خدمات).
4. **وسائل الارتكاب:** تشمل البرمجيات، التطبيقات، الحوسبة السحابية، ومنصات التواصل، ويُعد توفير أدوات التزييف بقصد إجرامي فعلاً مساعداً في بعض التشريعات[3].

---

[1] European Union, Regulation (EU) 2024/1689 (Artificial Intelligence Act), Articles 50 and 99, Official Journal of the European Union, 2024, available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj

[2] صابرين جاسم مكطوف، أميل جبار عاشور، مرجع سابق، ص 90.

[3] علاء الدين منصور مغايرة، مرجع سابق، ص 137.

هذا وأن جرائم التزييف العميق قد تتخذ صورة جرائم مادية متعددة، إذ يمكن أن يُنتج الجاني المحتوى ثم ينشره ثم يبتز الضحية، وكل فعل قد يشكل جريمة مستقلة أو جريمة واحدة مركبة بحسب نظرة المشرع[1].

ثانياً: الركن المعنوي (القصد الجنائي)

يتطلب القصد الجنائي في جرائم التزييف العميق—كقاعدة عامة—القصد العام المتمثل في علم الجاني بأن المحتوى مزيف وإرادته إحداث النتيجة المحظورة (الإضرار بالسمعة، الحصول على منفعة، التضليل)، وفي بعض الصور يُشترط القصد الخاص، كالقصد الانتقامي في الإباحية الانتقامية، أو القصد الاحتيالي في جرائم النصب.

ويتصاعد الإشكال عند استخدام الذكاء الاصطناعي ذاته في إنتاج المحتوى دون تدخل بشري مباشر، فمن يتحمل المسؤولية مبرمج النموذج، أم مستخدمه، أم المنصة؟ وتذهب الاتجاهات القانونية المعاصرة إلى أن المسؤولية الجنائية تبقى إنسانية، وأن الذكاء الاصطناعي أداة لا شخصية قانونية[2]. وعليه، يُسأل الشخص الذي استخدم التقنية بقصد إجرامي، أو الذي أتاحها مع علمه باستخدامها المخالف.

أما الخطأ الجنائي فنادر التطبيق في هذه الجريمة، لأن إنشاء فيديو مزيف لشخص بعينه يفترض وعياً بالتعديل، إلا إذا أثبت الفاعل أنه اعتقد مشروعية الاستخدام (مثل العمل الفني أو السخرية)، وهو ما يفرض على المشرع تحديد استثناءات واضحة.

وتتعدد صور المسؤولية الجنائية في التزييف العميق بحسب دور الفاعل[3]:

1. **المسؤولية المباشرة**: يتحملها من أنشأ المحتوى المزيف بقصد إجرامي ونشره أو أتاحه للغير.
2. **المسؤولية عن المشاركة**: تشمل من ساهم في التزييف (مبرمج، مصمم نموذج، مزود خادم) إذا توافر لديه القصد والعلم بالاستخدام الإجرامي.
3. **مسؤولية المنصات**: محل خلاف فقهي، فالبعض يرى مسؤوليتها مدنية وإدارية عند التقصير في الإزالة، والبعض يميل إلى مسؤوليتها الجنائية عند المساهمة العمدية في النشر، ويُستحسن اعتماد مبدأ وسيط يُلزم المنصة بالإزالة الفورية بعد إشعار رسمي، دون تحميلها مسؤولية جنائية إلا عند العلم المسبق والتستر.

وفي السياق العراقي، تنص المادة (47) من قانون العقوبات على مسؤولية الشريك والمحرض والميسر، ما يتيح—نظرياً—متابعة من يوفر أدوات التزييف أو يحرض على استخدامها، شريطة إثبات القصد الجنائي المشترك، غير أن تطبيق هذه الأحكام على البيئة الرقمية يظل نادراً لغياب البنية التحتية للتحقيق الرقمي.

---

(1) سحر فؤاد مجيد النجار، مرجع سابق، ص 585.

(2) Simon Chesterman, "Artificial Intelligence and the Limits of Legal Personality", International & Comparative Law Quarterly, Vol. 69(4), 2020, pp. 10.

(3) سحر فؤاد مجيد النجار، مرجع سابق، ص 586. كذلك: علاء الدين منصور مغايرة، مرجع سابق، ص 137.

أما فيما يخص الضحية فإن جريمة التزييف العميق قد تكون جريمة فعلية أو جريمة خطر بحسب النظرة الفقهية، إذ يكفي في بعض التشريعات تحقق الخطر الجدي على السمعة دون انتظار وقوع الضرر المادي، خاصة في صور الإباحية الانتقامية حيث يستحيل إصلاح الضرر المعنوي بعد الانتشار الواسع[1].

المبحث الثالث

التحديات القانونية وسبل المواجهة

تُواجه جريمة التزييف العميق مجموعة من التحديات القانونية المعقدة التي تنبع من طبيعتها التقنية المتطورة، وما تثيره من صعوبات في الكشف والإثبات أمام القضاء الجنائي، فضلاً عن محدودية النصوص التشريعية التي تنظم هذا النوع المستحدث من الجرائم، وقد أدى ذلك إلى ظهور فجوة واضحة بين التطور التكنولوجي السريع وبين بطء الاستجابة التشريعية، مما يجعل من الصعب إحكام السيطرة القانونية على هذه الجريمة، وانطلاقاً من ذلك، يقتضي البحث تحليل أبرز الإشكالات القانونية والإثباتية التي تعترض مواجهة التزييف العميق، ثم بيان الآليات القانونية والتقنية الممكنة لتعزيز الحماية الجنائية، سواء من خلال تطوير التشريعات أو الاعتماد على الأدلة الرقمية والتقنيات الحديثة في كشف هذا النوع من الجرائم. وعلى وفق الآتي:

المطلب الأول

الإشكالات القانونية والإثباتية

تُعد الإشكالات القانونية والإثباتية من أبرز التحديات التي تثيرها جريمة التزييف العميق، إذ يصعب في كثير من الحالات التحقق من صحة المحتوى الرقمي وتمييزه عن المحتوى الحقيقي، خاصة مع التطور الكبير في تقنيات الذكاء الاصطناعي. كما أن غياب نصوص قانونية صريحة ومحددة في بعض التشريعات، ومنها التشريع العراقي، يزيد من صعوبة تكييف هذه الأفعال وإثباتها أمام القضاء، مما يضعف من فعالية الحماية الجنائية.

أولاً: صعوبة إثبات التزييف العميق أمام القضاء

يمثل إثبات التزييف العميق أحد أبرز التحديات أمام القضاء الجنائي. فعلى جانب الادعاء، يجب إثبات أن المحتوى مزيف وليس حقيقياً، وهو ما يستلزم خبرة تقنية وبرامج كشف متخصصة (مثل تحليل عدم الاتساق في الإضاءة، أو اكتشاف آثار الخوارزميات)، وعلى جانب الدفاع، قد يدفع المتهم بأن المحتوى حقيقي، فيحتاج القضاء إلى تقرير خبير رقمي معتمد. وتتفاقم المشكلة عند استخدام التزييف العميق في الإثبات الجنائي ذاته، إذ يمكن تزييف مقاطع تُقدم كدليل، أو تزييف شهادات مرئية، مما يهز الثقة في الأدلة الرقمية ويستدعي معايير جديدة لقبولها[2]. وهذا ما يدفع بضرورة تطوير إطار قانوني للأدلة الرقمية يتضمن آليات التحقق من أصالة المحتوى متعدد الوسائط[3].

---

(1) سحر فؤاد مجيد النجار، مرجع سابق، ص 587.

(2) اياد عبد حمزة بعيوي، مرجع سابق، ص 345-348

(3) نورهان محمد الربيعي، التحقيقات القضائية الجنائية في ظل الذكاء الاصطناعي: دراسة مقارنة، مجلة آشور للعلوم القانونية والسياسية، المجلد 2، العدد 4، 2025، ص 1010.

كما أن الطابع العابر للحدود يعقد الإثبات، إذ قد يكون الجاني والخادم والضحية في دول مختلفة، مما يفرض التعاون القضائي الدولي وتبادل الأدلة وتطبيق نظام تسليم المجرمين.

ثانياً: قصور التشريعات الجنائية الحالية

يتجلى قصور التشريع العراقي في معالجة الجرائم المعلوماتية بما في ذلك جرائم التزييف العميق محاور متعددة، مثل غياب تعريف التزييف العميق أو الذكاء الاصطناعي في قانون العقوبات، وتأخر إصدار قانون الجرائم المعلوماتية، ما يترك الفضاء الرقمي دون تنظيم جزائي متخصص، واقتصار التكييف على جرائم التشهير والتزوير التي لا تغطي إنشاء المحتوى دون نشره، ولا تعالج التزييف غير التشهيري (كالاحتيال الانتخابي). وكذلك غياب عقوبات متناسبة مع خطورة الجريمة واتساع انتشارها.

وللمقارنة، يوفر القانون المصري في المواد (25) و(26) من قانون (175) لسنة 2018 إطاراً أوسع لمعاقبة من ينشر معلومات أو صوراً تمس الخصوصية أو السمعة باستخدام تقنية المعلومات، مع عقوبات بالحبس والغرامة[1]. أما الإمارات فتشدد العقوبة في المادة (44) من المرسوم (34) لسنة 2021 عند استخدام التقنية للتشهير، بعقوبة الحبس سنة على الأقل وغرامة (250,000 – 500,000) درهم[2]. وفرنسا تجرم النشر دون موافقة صريحة سواء توفر قصد جرمي ام لا، أما الاتحاد الأوروبي فقد نظم التزييف عبر قانون الذكاء الاصطناعي (AI Act) بفرض إفصاح إلزامي عن المحتوى الاصطناعي، مع غرامات إدارية كبيرة، دون إنشاء جريمة جنائية موحدة على مستوى الاتحاد[3].

إن قصور التشريع العراقي عن معالجة جرائم المعلوماتية بصورة عامة لا يقتصر على غياب التعريف، بل يمتد إلى غياب سياسة جنائية متكاملة تجمع بين الردع والوقاية، حيث ترى الباحثة أن المشرع الجزائي مطالب بإعادة تكييف القواعد القانونية ذات المدلول الواقعي المادي للتعامل مع واقع افتراضي غير ملموس، والاهتمام بسياسات المنع والوقاية لا العقاب وحده، إذ إن غياب نصوص صريحة يجعل الجاني قد يفلت من العقاب رغم جسامة الأضرار، خاصة أن هذه الجرائم بما في ذلك التزييف العميق جرائم عابرة للحدود وتتطلب تعاوناً دولياً.

ومن الإشكالات الإثباتية المرتبطة بالقصور التشريعي غياب قانون عراقي للأدلة الإلكترونية يحدد معايير قبول المحتوى الرقمي وآليات التحقق من أصالته، إذ إن التزييف العميق يهدد مفهوم الثقة في المحتوى الرقمي، ويضع المشرع أمام معضلة إيجاد إطار قانوني يحمي الحقوق دون إعاقة الابتكار، كما أن سرعة تطور التقنية تفوق سرعة التشريع، ما يستدعي تشريعاً مرناً قابلاً للتحديث بموجب مراسيم أو لوائح تنفيذية.

المطلب الثاني

آليات الحماية والمواجهة القانونية

---

[1] المواد (25) و (26) من قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018.

[2] المادة (44) من المرسوم بقانون اتحادي إماراتي رقم (34) لسنة 2021.

[3] European Union, Regulation (EU) 2024/1689 (Artificial Intelligence Act), op.cit.

في ظل التحديات التي تفرضها جريمة التزييف العميق، تبرز الحاجة إلى تبني آليات قانونية وتقنية فاعلة للحد من آثارها، ويشمل ذلك تطوير التشريعات الجنائية بما يتناسب مع طبيعة الجرائم المعلوماتية الحديثة، إلى جانب تعزيز دور الأدلة الرقمية والتقنيات المتقدمة في كشف التزييف، بما يضمن تحقيق التوازن بين التطور التكنولوجي ومتطلبات الحماية القانونية والعدالة الجنائية.

أولاً: الحلول التشريعية المقترحة وتحديث القوانين

إن من اول وأهم الحلول التشريعية الواجب اتخاذها في مواجهة جريمة التزييف العميق هو اعتماد قانون جنائي خاص بالجرائم المعلوماتية، يتضمن تعريفاً صريحاً للتزييف العميق، وجرائم إنشائه ونشره والتحريض عليه، وعقوبات متدرجة بحسب جسامة الضرر (تشهير، ابتزاز، احتيال، مساس بالأمن الوطني).

كما أن من الحلول التشريعية لمواجهة جريمة التزييف العميق هو اعتماد نظام إلزامية الإفصاح، والذي بموجبه يلتزم من ينشر محتوىً مُولَداً بالذكاء الاصطناعي بالإشارة الصريحة إلى طبيعته، وقد التفت قانون الاتحاد الأوربي الى هذا النظام واعتمده في المادة (50) من قانون الاتحاد الأوروبي للذكاء الاصطناعي.

وفضلاً عن السابق، فأن تحديد مسؤولية منصات النشر عن إزالة المحتوى المزيف بعد الإبلاغ، دون إعفائها من المساءلة الجنائية عند المساهمة العمدية هو توجه تشريعي حديث في مواجهة الجرائم المعلوماتية وخاصة جريمة التزييف العميق، وهذا التوجه يعكس سياسية جنائية علاجية ووقائية تحد من انتشار هذه الجرائم.

ثانياً: دور الأدلة الرقمية والتقنيات الحديثة في كشف التزييف

لا تكتمل المسؤولية الجنائية دون آليات إثبات فاعلة تشمل مجموعة من الأدوات الحديثة سواء على الصعيد التقني او القانوني، مثل:

- **تقنيات الكشف**: برامج تحلل التماسك البصري، والومضات، والتناسق الصوتي، وتُستخدم في التحقيقات الجنائية[1].
- البيانات الوصفية: وتتمثل في اعتماد اليات لتوليد بيانات وصفية لكل محتوي يتم نشره ليسهل الوصول له والتحقق من صحته ومحتواه وبشكل سريع.
- **التوقيع الرقمي والعلامات المائية**: وتتمثل باعتماد أنظمة ملزمة للجهات الإعلامية او الشخصيات العامة او غيرها بإضافة علامة مائية وتواقيع رقمية على المحتوى المنشور من قبلهم، يحمي هذ المحتوى ويمنع تزويره او التلاعب به، مما يسهم في إثبات أصالة المحتوى المنشور رسمياً، والوقاية من تزيفه.

وعلى المستوى الإجرائي، فأن من الحلول التي تسهم في مواجهة جريمة التزييف العميق، وتسهل من استخدام التنقيات الحديثة كأدلة اثبات، هي إدخال إجراءات خاصة في مسار التحقيق والمحاكمة، منها إلزام النيابة العامة

[1] محمد كرم كمال الدين الصاوي، تكنولوجيا التزييف العميق: دراسة بحثية حول الجوانب المظلمة للذكاء الاصطناعي، مجلة العمارة والفنون والعلوم الإنسانية، المجلد 10، العدد 51، 2025، ص 674.

بإرفاق تقرير خبير رقمي مع كل دعوى تتعلق بمحتوى مرئي أو سمعي مشكوك في أصالته، وتمكين المحكمة من طلب إعادة فحص الدليل في أي مرحلة، واعتماد سجل زمني لحظة ضبط المحتوى الرقمي، وتحديد مدة معقولة لإزالة المحتوى المزيف من المنصات بعد صدور أمر قضائي[1]. وكذلك إنشاء قاعدة بيانات وطنية للمحتوى المُثبت تزييفه، تُستخدم كمرجع للتحقيقات المستقبلية دون الإخلال بحقوق الضحايا في الخصوصية.

الخاتمة

إن جريمة التزييف العميق تمثل تحولاً بنيوياً في ممارسة الجريمة، يفرض إعادة صياغة قواعد المسؤولية الجنائية، إذ إن التزييف العميق يختلف جوهرياً عن التزوير التقليدي في الفعل المستهدف والوسيلة والغاية، ما يجعل التكييف التقليدي كافياً جزئياً لا كلياً، ويعاني التشريع العراقي من فراغاً تشريعياً في معالجة هذه الجريمة على وجه الخصوص والجرائم المعلوماتية على وجه العموم، مما يدفع القضاء العراق بالاحتكام إلى نصوص جنائية في قانون العقوبات تخص جرائم تقليدية احكامها وعقوبتها لا تتناسب مع طبيعة الجرائم المعلوماتية .

الاستنتاجات

1. التزييف العميق جريمة معلوماتية مستقلة في مضمونها، تختلف عن التزوير التقليدي في الفعل والوسيلة والنتيجة.
2. القانون العراقي يفتقر إلى نص صريح يجرم التزييف العميق، ويُلجأ في ممارسته إلى تكييفات متفرقة في قانون العقوبات.
3. أركان المسؤولية الجنائية في جريمة التزييف العميق تتطلب تحديداً دقيقاً للفعل (الإنشاء/النشر) والقصد (الإضرار/الاحتيال) والوسيلة التقنية، ولكن يبقى الإثبات الجنائي يمثل العائق الأبرز في معالجة هذه الجريمة، ويتطلب خبرة رقمية وإطاراً قانونياً للأدلة الإلكترونية.

التوصيات

1. الإسراع بإصدار قانون الجرائم المعلوماتية العراقي وتضمينه تعريفاً صريحاً للتزييف العميق وعقوباته.
2. تعديل قانون العقوبات أو قانون الإثبات لاستيعاب الأدلة الرقمية ومعايير التحقق من أصالة المحتوى.
3. إنشاء وحدات خبرة رقمية في الادعاء العام والقضاء للتحقيق في جرائم التزييف العميق.
4. تعزيز التعاون الدولي والانضمام إلى الاتفاقيات الإقليمية لمكافحة الجرائم السيبرانية.

قائمة المصادر

أولاً: المصادر باللغة العربية

الأبحاث والمجلات العلمية

[1] اياد عبد حمزة بعيوي، مرجع سابق، ص 350.

1. إياد عبد حمزة بعيوي، "الإطار القانوني لمكافحة جرائم التزييف العميق وأثره على الإثبات الجنائي"، مجلة آشور للعلوم القانونية والسياسية، المجلد 3، العدد 1، 2026.
2. رباب مصطفى عبد المنعم الحكيم، "الجوانب القانونية للتزييف العميق"، مجلة الحقوق، جامعة الأزهر، العدد 48، 2025.
3. رضا إبراهيم عبدالله البيومي، "الحماية القانونية من مخاطر التزييف العميق في الفقه الإسلامي والقانون الوضعي"، مجلة روح القانون، جامعة طنطا، المجلد 35، العدد 102، 2023.
4. سحر فؤاد مجيد النجار، "المواجهة الجنائية للجرائم الناشئة عن استخدام تقنية التزييف العميق"، مجلة العلوم القانونية، المجلد 39، العدد الثاني، 2024.
5. صابرين جاسم مكطوف، وأميل جبار عاشور، "الأحكام الموضوعية لجريمة التزييف العميق ومعالجتها القانونية (دراسة مقارنة)"، مجلة آشور للعلوم القانونية والسياسية، المجلد 2، العدد 2، 2025.
6. علاء الدين منصور مغايرة، "جرائم الذكاء الاصطناعي وسبل مواجهتها: جرائم التزييف العميق نموذجًا"، المجلة الدولية للقانون، جامعة قطر، المجلد 13، العدد 2، 2024.
7. محمد كرم كمال الدين الصاوي، "تكنولوجيا التزييف العميق: دراسة بحثية حول الجوانب المظلمة للذكاء الاصطناعي"، مجلة العمارة والفنون والعلوم الإنسانية، المجلد 10، العدد 51، 2025.
8. نورهان محمد الربيعي، "التحقيقات القضائية الجنائية في ظل الذكاء الاصطناعي: دراسة مقارنة"، مجلة آشور للعلوم القانونية والسياسية، المجلد 2، العدد 4، 2025.

2. القوانين والتشريعات

1. قانون العقوبات العراقي رقم (111) لسنة 1969 (المعدل).
2. قانون مكافحة جرائم تقنية المعلومات المصري رقم (175) لسنة 2018.
3. المرسوم بقانون اتحادي (إماراتي) رقم (34) لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية.

3. المصادر الإلكترونية

1. صفاء عياد، "قانون جرائم المعلوماتية في العراق"، بحث منشور على الإنترنت، 2022، (تاريخ آخر زيارة 2026/6/10)، متاح على الرابط: https://smex.org/iraqi-cybercrime-draft-law-in-suspension
2. هشام كاظم، "توسيع الاشتباه بدل التنظيم.. قراءة قانون الجرائم الإلكترونية في العراق"، بحث منشور على الإنترنت، 2024، (تاريخ آخر زيارة 2026/6/10)، متاح على الرابط: https://jummar.media/11958

ثانياً: المصادر باللغة الأجنبية

A- (Articles & Papers)

- Chesney, B., & Citron, D., "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security", California Law Review, Vol. 107, 2019.
- Chesterman, Simon, "Artificial Intelligence and the Limits of Legal Personality", International & Comparative Law Quarterly, Vol. 69(4), 2020.
- Goodfellow, I. J. et al., "Generative Adversarial Nets", Proceedings of the 28th Annual Conference on Neural Information Processing Systems (NeurIPS), 2014.

B- Foreign Legislation

- European Union, Regulation (EU) 2024/1689 (Artificial Intelligence Act),
- French Penal Code (Code pénal français),

C- Online Resources

- Baker McKenzie, "United Arab Emirates: Deepfakes and the Use of Artificial Intelligence (AI)", 11 June 2024. Available at: https://insightplus.bakermckenzie.com
- Damiani, J., "A Voice Deepfake Was Used to Scam a CEO Out of $243,000", Forbes, 2019. Available at: https://www.forbes.com
- Shivangi, A., "15 Best Deepfake Apps & Websites that You Must Try", Smartprix, 2023. Available at: https://www.smartprix.com