مجـــلـة الحـــق للعلوم الشرعية والقانونية
Al-haq Journal for Sharia and Legal Sciences
تصدر عن كلية القانون – جامعة بني وليد – ليبيا
Website: https://www.al-haqjournal.ly/index.php/alhaq/index
المجلد الثالث عشر ــ العدد الأول 2026 ــ الصفحات (473-484)
ISSN 3005 – 3919 معامل التأثير العربي 1.72 لسنة 2025 2.113 (ISI) لسنة 2025

Artificial Intelligence Crimes the Crime of Deep fake a model.

Abdelnnaser Masoud Ahmed Alforti *
Department of Criminal law, Faculty of law, Azzaytuna University, Tarhuna, Libya
a.alforte@azu.edu.ly

جرائم الذكاء الاصطناعي
(جريمة التزييف العميق نموذجًا)

عبد الناصر مسعود أحمد الفورتي*
قسم القانون الجنائي، كلية القانون، جامعة الزيتونة، ترهونة، ليبيا.

Received: 06-02-2026	Accepted: 22-03-2026	Published: 28-03-2026

Copyright: © 2026 by the authors. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (https://creativecommons.org/licenses/by/4.0/).

الملخص:
يأتي هذا البحث في ظل التطور المتسارع لتقنيات الذكاء الاصطناعي وكثرة استعمالها على نطاق واسع من قبل مختلف فئات المجتمع، حيث يهدف هذا البحث إلى تسليط الضوء على نوع من الجرائم يتم تكييفها على أنها من بين جرائم الذكاء الاصطناعي ويطلق عليها جرائم التزييف العميق، وهي من الجرائم الحديثة في مجال العلوم الجنائية، وتتمثل مشكلة البحث في معرفة ماهية التزييف العميق وما ينتج عنه من مخاطر ناهيك عن بيان مدى ملاءمة النصوص الجنائية الحالية على هذا النوع من الجرائم، وقد اعتمد الباحث على المنهج التحليلي والاستقرائي وكذلك المنهج الوصفي، مُختتمًا البحث بعدة نتائج أهمها: أن التزييف العميق تقنية تعتمد بشكل أساسي على الذكاء الاصطناعي وهذا أهم عامل خطورة يُميزها.
وقد كان قانون الجرائم الالكترونية قاصرًا على استيعاب جرائم التزييف العميق وكذلك توصلنا إلى أن ما يميز جرائم التزييف العميق عن التزييف العادي هو أن الأول يستخدم أدوات تحرير بسيطة، لذلك أوصينا بإنشاء قانون ينظم جرائم الذكاء، فقد أصبحت حاجة ضرورية.

الكلمات الدالة: الابتزاز الالكتروني، التزييف العميق، الدليل الالكتروني، الذكاء الاصطناعي، قانون الجرائم الالكترونية.

Abstract:
This study is conducted in light of the rapid advancement of artificial intelligence technologies and their extensive adoption across various segments of society. It aims to examine a category of crimes associated with artificial intelligence, specifically deepfake crimes, which are considered among the emerging forms of criminality within the field of criminal sciences. The research problem centers on defining the concept of deepfakes and identifying the risks arising from their use, in addition to assessing the adequacy of existing criminal legal frameworks in addressing this type of offense. To this end, the study adopts analytical, inductive, and descriptive methodologies. The findings of the study indicate that deepfake technology is fundamentally

dependent on artificial intelligence, which constitutes the primary factor contributing to its severity and potential harm.
Furthermore, the study reveals that current cybercrime legislation remains inadequate to comprehensively address deepfake related offenses. It also highlights that what distinguishes deepfake crimes from traditional forms of forgery is their reliance on relatively simple digital editing tools. Accordingly, the study recommends the enactment of a dedicated legal framework to regulate artificial intelligence related crimes, given the pressing need for such legislation in light of ongoing technological developments.

Keywords: Deepfake Technology; Artificial Intelligence; Cybercrime Legislation; Cyber Extortion; Digital Evidence.

المُقَدِّمَة:

مع ظهور الذكاء الاصطناعي وتطوره، ظهر معه ما يعرف بتقنية التزييف العميق والتي تقوم أساسًا على التلاعب بالصور ومقاطع الفيديو والأصوات باستخدام أدوات التعلم العميق، حيث يمكن لهذه التقنية استبدال الوجوه داخل مقاطع الفيديو وتغيير الحديث مع المحافظة على نفس الصوت بكل سهولة وبشكل يقترب من الحقيقة؛ مما فتح معه أبوابًا عديدة لمختلف الجرائم كالابتزاز والتشهير والانتقام الإباحي والتزوير والاحتيال وغيرها، والتي تشكل تحديًا جديدًا بالنسبة إلى التشريعات الحالية.

أولًا: مشكلة البحث:

تتمثل إشكالية البحث في مدى كفاية نصوص قانون الجرائم الإلكترونية الليبي في مواجهة الجرائم الناجمة عن التزييف العميق للحد من هذه الجرائم من عدمها؟ وكذلك بيان مفهوم هذه التقنية ومخاطرها؟ وما الفرق بين التزييف العميق والتزييف الالكتروني العادي؟ ما مدى إمكانية مواجهة أفعال التزييف العميق في ظل مبدأ الشرعية؟ وكيفية تأثير هذه التقنية على الدليل الجنائي؟

ثانيًا: أهمية الموضوع:

تكمن قيمة هذا الموضوع في كونه يتناول أحد الموضوعات الحديثة والمستجدة، حيث يناقش ظاهرة جديدة على المجتمع وعلى تشريعاتنا، فيستعرض النصوص الجنائية الحالية ويبين أوجه القصور فيها؛ الأمر الذي يساهم في تطوير القوانين المتعلقة بالذكاء الاصطناعي في المستقبل.

ثالثًا: الهدف من الدراسة:

1. إثراء البحث العلمي القانوني عبر مناقشة مواضيع حديثة وتمس المجتمع.
2. الوصول إلى تعريف قانوني دقيق لجرائم التزييف العميق.
3. معرفة مدى قدرة القانون رقم 5 لسنة 2022 بشأن الجرائم الالكترونية على التصدي لجرائم التزييف العميق.
4. معرفة الفرق بين التزييف العميق والتزييف الالكتروني العادي.
5. بيان كيفية تأثير تقنية التزييف العميق على الدليل الجنائي وآلية مواجهة ذلك.

رابعًا: منهجية البحث:

يتبنى هذا البحث المنهج التحليلي والاستقرائي للنصوص القانونية ذات الصلة بالموضوع والمنهج الوصفي، ويكون نطاق البحث محصورًا في التشريع الليبي فقط.

خامسًا: خطة البحث:

المطلب الأول: مفهوم جريمة التزييف العميق وتمييزها عن غيرها من الجرائم

الفرع الأول: تعريف التزييف العميق ومخاطره

الفرع الثاني: التمييز بين التزييف العميق والتزييف الإلكتروني العادي

المطلب الثاني: تقنية التزييف العميق في ضوء مبدأ الشرعية الجنائية ومدى تأثير هذه التقنية على الدليل الرقمي

الفرع الأول: تقنية التزييف العميق في ضوء مبدأ الشرعية الجنائية

الفرع الثاني: قيمة الدليل الرقمي في ظل تقنية التزييف العميق

الخاتمة.

المطلب الأول: مفهوم جريمة التزييف العميق وتمييزها عن غيرها من الجرائم

تمهيد وتقسيم:

شكلت تقنية التزييف العميق (Deep Fake) قلقًا كبيرًا في الآونة الأخيرة للمجتمعات والحكومات، وخاصةً مع تنامي التطبيقات والأدوات الرقمية الحديثة وتعاظم دورها في الحياة الافتراضية، إذ يعد التزييف العميق أحد أسباب الأساليب العدائية المستخدمة ضد الأفراد أو الأشخاص المعنوية؛ لغرض الإضرار بسمعتها أو تضليل الرأي العام، ونتناول في هذا المطلب تعريف التزييف العميق وأهم المخاطر لهذه التقنية وهذا في الفرع الأول، أما الفرع الثاني فيتطرق إلى مسألة التمييز بين جريمة التزييف العميق وجريمة التزييف الالكتروني العادي.

الفرع الأول: تعريف التزييف العميق ومخاطره

تكمن أهمية الضبط الاصطلاحي القانوني عمومًا في منع اللبس وإزاحة الغموض والإبهام عن مصطلح ما، وتزداد أهميته إذا كان ذلك المُصطلح مُستحدثًا، كما تكمن العبرة في مدى مشروعية استخدام تقنية التزييف العميق من عدمه في الغرض والنتيجة، أي نية التضليل أو تحقق الغرض، فليس كل تزييف عميق يعتبر غير مشروع، والعكس صحيح إذا استُخدم في أغراض التعليم والبحث العلمي، بالتالي نسعى في هذا الفرع جاهدين إلى محاولة تعريف مصطلح التزييف العميق البند أولًا، واستخلاص أهم المخاطر التي يُشكلها من صميم ذلك التعريف في البند ثانيًا.

أولًا: تعريف التزييف العميق:

يعرف التزييف العميق (Deep Fake) على أنه مقطع فيديو تم إنشاؤه بقصد الخداع، ويبدو أنه يصور شخصًا حقيقيًا يقوم بفعل لم يحدث في الواقع (البرنامج الوطني للذكاء الاصطناعي دليل التزييف العميق ،2021، ص5)

وقد عرف أيضًا على أنه (العملية التي يجري فيها استبدال الوجه (Faceswapping) باستخدام تقنيات الذكاء الاصطناعي وتعلم الآلة، وذلك من خلال تدريب خوارزميات الذكاء الاصطناعي على الصور المستخرجة من شبكات منفصلة، ثم إعادة بناء الوجه الجديد وإنشاء المقاطع المرئية المطلوبة، كما يمكن تنفيذ العملية نفسها لإنشاء مقاطع صوتية (محرم، 2022، ص2529)

وقد عرفه برلمان الاتحاد الأوروبي بأنه عبارة عن وسائط صوتية أو بصرية معدلة أو مصطنعة تبدو حقيقية، وتصور شخصًا أو أشخاصًا يظهرون وكأنهم يقولون أو يفعلون شيئًا لم يقولوه أو يفعلوه أبدًا، ويتم إنتاجه باستخدام تكنولوجيا الذكاء الاصطناعي بما في ذلك التعلم الآلي والتعلم العميق (مغايرة، 2024، ص133)

ومن خلال التعريفات السابقة نجد أنها ركزت في تعريفها للتزييف العميق على الخصائص التقنية، في حين أن بعضها لم يذكر كافة الوسائط المُحتمل وقوع عملية التزييف بشأنها، وتأسيسًا على ذلك، فإنه يمكننا أن نعرف جريمة التزييف العميق- حسب رؤيتنا- على أنها (العملية التي يتم فيها إدخال وسائط الكترونية معينة (صور أو فيديوهات أو أصوات أو نصوص) عبر أدوات أو برامج أو تطبيقات تعتمد على الذكاء الاصطناعي لكي يتم تغييرها أو إعادة بنائها من جديد بشكل كلي أو جزئي؛ وذلك بقصد الإضرار بالغير أو تحقيق ربح مادي أو معنوي).

ومن خلال التعريف السابق نلاحظ أن جريمة التزييف العميق تقوم على أساسات تقنية لازمة؛ لكي تتم هذه الجريمة نذكرها فيما يلي:

1. ضرورة وجود مدخلات الكترونية يتم عليها التعديل أو البناء مثل الصور أو الفيديوهات أو الأصوات أو النصوص، وغالباً ما يقوم الأشخاص بنشر هذه البيانات على نطاق واسع في وسائل التواصل الاجتماعي بشكل عام، والعلاقة طردية، فكلما ازداد حجم البيانات التي يحصل عليها صانع مقاطع الصوت أو الفيديو المزيفة، تحسنت جودتها وأصبحت أقرب إلى الواقع (البرنامج الوطني للذكاء الاصطناعي دليل التزييف العميق، 2021، ص12) ووجبت الإشارة إلى عدم حاجة الأجيال الجديدة من برامج التزييف العميق لأحجام كبيرة من البيانات لكي تتم عملها.
2. وجود برامج أو تطبيقات مدعومة بالذكاء الاصطناعي:

فتقنية التزييف العميق تعتمد بشكل أساسي على الذكاء الاصطناعي للتلاعب بالصور أو الفيديوهات أو الأصوات، إذ تعمل بشبكة تسمى شبكة الخصومة التوليدية التي تعد نموذجًا للتعلم الآلي، حيث تتنافس شبكتان عصبيتان ضد بعضهما من أجل الخروج بنتائج أكثر دقة، حيث تقوم الشبكة الأولى والتي تسمى المولد(Generator) بإنشاء صورة أو مقطع فيديو مزيف ثُم يطلب من الشبكة الثانية والتي تعرف بالمميز(discriminator) بتحديد ما إذا كان المقطع حقيقيًا أم مزيفًا، وعليه فإذا اكتشفت الشبكة الثانية أن المقطع مزيف، فإنها تعطي إشارة إلى الشبكة الأولى للمحاولة مرة أخرى والتي تحاول من جديد بعد أن تعلمت من الشبكة الثانية مالا يجب فعله عند إنشاء المقطع أو الصورة، وعلى هذا الأساس تتحرك كلتا الشبكتين للوصول إلى أفضل نتيجة وقريبة من الواقع (2022,thought leadership)

واستنادًا إلى ما سبق نجد أن للذكاء الاصطناعي خاصية خطيرة تتمحور حول قدرته على التعلم من أخطائه والقدرة على التحسين الدائم وبناء خبرات من الأخطاء السابقة، وهذه الخاصية في إطار جريمة التزييف العميق تشكل عقبة كبيرة، فهي تجعل التزييف أكثر واقعية وأصعب في الكشف، مما يدفعنا إلى القول بأن لهذه التقنية مخاطر عدة على مستويات مختلفة.

ثانيًا: مخاطر تقنية التزييف العميق

نظرًا للتطور السريع في تقنية التزييف العميق وسهولة الوصول إليها أسهم ذلك في وصول ضعاف النفوس لهذه التقنية واستخدامها بشكل يضر الأفراد والمجتمع والدولة وفيما يلي سنعرض أوجه هذه المخاطر وأبرز الجرائم المتولدة عن هذه التقنية، ومدى قدرة القانون رقم 5 لسنة 2022م المتعلق بالجرائم الالكترونية على استيعاب جرائم هذه التقنية من عدمه.

1. **جرائم الابتزاز والانتقام الإباحي العميق:**

من الممكن توظيف هذه التقنية لتشويه سمعة الأفراد وإثارة الثغرات الطائفية بين أفراد المجتمع وخلق مشاكل اجتماعية تؤدي إلى زعزعة استقرار المجتمع، حيث يستخدم أصحاب النفوس المريضة تقنية التزييف العميق لتنفيذ مآربهم الإجرامية باستغلال ضعف الشخص المستهدف وخصوصًا الإناث وتنفيذ الابتزاز؛ للحصول على منافع مادية أو معنوية، حيث يقوم الجاني بإنتاج صور أو فيديو يسيء للضحية لجعله يستسلم لرغبات ومآرب المجرم وهو ما يُعرف بجرائم الابتزاز (مغايرة، ص136)

يُمكننا القول أن المُتمعن في نصوص القانون رقم 5 لسنة 2022م بشأن الجرائم الالكترونية، يجد أنه لم ينص بشكل مباشر على جريمة الابتزاز الالكتروني، غير أن المشرع الليبي حاول الإحاطة بهذه الجريمة بعدة نصوص، كنص المادة (19) المتعلق بإنتاج المواد الإباحية وترويجها، وكذلك نص المادة (21) المتعلق بمزج أو تركيب الصوت والصور، حيث نرى أن هذه المواد لم تستوعب بشكلٍ كافٍ جرائم التزييف العميق، نوضح ذلك كالآتي:

1. نصت المادة 19 على المعاقبة بالحبس وبغرامة لا تقل عن (1000) ألف دينار ولا تزيد عن (10000) عشرة آلاف دينار كل مَن:

1- أنتج لغيره مواد إباحية بقصد توزيعها أو بثها عبر نظام معلوماتي (نص المادة 19 من القانون رقم 5 لسنة 2022 بشأن الجرائم الالكترونية)

نلاحظ في الفقرة السابقة أن المشرع استعمل مصطلح (أنتج) الذي يشير إلى العملية التقليدية حيثما تتم صناعة المحتوى الإباحي بما في ذلك التصوير واستعمال أشخاص حقيقيين وكاميرات وأجهزة أخرى، وتشمل هذه العملية الإخراج والتصوير والمونتاج، في حين أن جرائم التشهير والابتزاز الالكتروني التي تستخدم تقنية التزييف العميق تخرج من دائرة التجريم؛ وذلك لأن هذه التقنية تقوم بتوليد صور أو فيديوهات إباحية من مواد سليمة وغير إباحية، فمصطلح التوليد هنا يعنى إنشاء محتوى جديد بالكامل باستخدام الذكاء الاصطناعي ودون الاستعانة بأشخاص حقيقيين؛ مما يجعل نص المادة (19) غير متطابقة مع مثل هذا النوع من الجرائم .

ويلاحظ أن سياق الفقرة (1) من المادة (19) قد خلا من الإشارة إلى استخدام تطبيقات أو مواقع الكترونية لكي تتم بها عملية الإنتاج، وهذا ما يدعم قولنا أن نص المادة لا يدخل ضمن جرائم التزييف العميق وإنما يقتصر على الإنتاج فقط أي تصوير المواد الإباحية.

2 - نص المادة (21) والتي تحمل عنوان (مزج أو تركيب الصوت والصور)، حيث نصت على أنه:

"يعاقب بالحبس مدة لا تقل عن سنة كل من مزج أو ركب بغير تصريح مكتوب أو الكتروني من صاحب الشأن صوتًا أو صورةً لأحد الأشخاص باستخدام شبكة المعلومات الدولية أو أي وسيلة الكترونية أخرى بقصد الإضرار بالآخرين ما لم يكن ذلك مسموح به في القوانين المنظمة لعمل الصحافة والحقوق والحريات العامة، فإذا كان المزج أو التركيب مع صور أو أصوات إباحية ونشرها عبر شبكة المعلومات الدولية أو بأي وسيلة الكرتونية أخرى تكون العقوبة السجن مدة لا تقل عن خمس سنوات" (نص المادة 21 من القانون رقم 5 لسنة 2022 بشأن الجرائم الالكترونية)

نُلاحظ أنه للوهلة الأولى يمكن القول بأن نص هذه المادة قادر على معالجة جرائم التشهير أو الابتزاز الالكتروني المعتمدة على تقنية التزييف العميق غير أن بعض النقص والقصور اعتراها، فنجدها قد حددت الوسائط الالكترونية التي يشملها المزج أو التركيب الأصوات أو الصور وهذا يشكل خللًا في النص التشريعي، فجرائم التزييف العميق أوسع نطاقًا و أكثر تنوعًا في الأساليب المستخدمة، فلم ينص المشرع على الفيديوهات أو النصوص المكتوبة باعتبارها وسائط يمكن التلاعب بها والتعديل عليها بكل سهولة، ونرى أنه كان بإمكان المشرع الليبي تدارك هذه الإشكالية بإضافة عبارة فضفاضة (وأي وسائط أخرى) لجعل النص يستوعب جميع أنواع الوسائط المعروفة أو التي قد تستجد في المستقبل في ظل هذا التطور السريع.

2. جرائم الاحتيال والتزوير العميق:

يستخدم الجاني في مثل هذا النوع من الجرائم تقنية التزييف العميق لتقليد أصوات أو وجوه الأفراد الموثوق بهم بشكل مقنع؛ من أجل الحصول على معلومات حساسة أو خداع الضحايا ويكون ذلك عبر مكالمات احتيالية أو مكالمات عبر الفيديو، حيث تسهل تقنية التزييف العميق للجاني عملية التنكر في صورة شخصية تنفيذية أو ذات سلطة لغرض إجراء معاملات مالية (الهيئة السعودية للبيانات والذكاء الاصطناعي، مبادئ التزييف العميق ص6) أو قد يتم استخدام الرسائل المدمجة بالتزييف العميق، حيث يتم إرسال محتوى يتضمن معلومات مزيفة توحي بالموثوقية لتوجيه الضحايا إلى روابط ضارة أو طلبات تحويل مالية، قد تحتوي هذه الرسائل على مقاطع صوتية أو فيديوهات ملحقة تدعم مصداقية المحتوى وتزيد من احتمالية استجابة الضحية (التزييف العميق Deepfake في التصيد الالكتروني: التحديات والحلول، 2024).

ففي مارس عام 2019 استطاع بعض المجرمين خداع الرئيس التنفيذي لشركة بريطانية تعمل في مجال الطاقة لتحويل مبلغ 243 ألف دولار إلى مورد من دولة المجر عبر ملف صوتي مزيف (البيومي، مجلة روح القانون، عدد خاص، ص842) ، لم يتوقف خطر التزييف العميق عند الخسائر المادية للأفراد فحسب، بل تعدى ذلك إلى الإضرار بصحة الأفراد فيما يعرف بالاحتيال الطبي، ففي تحقيق -نشرته المجلة الطبية

البريطانية (BMJ) في يوليو 2024- كشف عن استخدام تقنية التزييف العميق لإنشاء مقاطع فيديو مزيفة تظهر أطباء بارزين في المملكة المتحدة يروجون لمنتجات مشكوك في مصداقيتها، حيث ظهرت فيديوهات لأحد الأطباء الإعلامين والذي يدعى (هيلاري جونز) وهو يروج لعقار يُستخدم في علاج ارتفاع ضغط الدم(خرواط، 2024) ومن زاوية أخرى، فإن وجود محتوى طبي مزيف يؤدي إلي هز ثقة العامة في الأطباء و انتشار المعلومات الطبية المتضاربة حتى لا يعرف ما هو صحيح
وما هو خاطئ.

وعند الاطلاع على قانون الجرائم الالكترونية الليبي نجد أنه لم ينص على جرائم الاحتيال الالكتروني أو التصيد الالكتروني، غير أن هذا القانون في مادته 49 نص على أنه ((في غير الجرائم المنصوص عليها في هذا القانون، يعاقب كل من ارتكب جريمة معاقبٌ عليها بموجب قانون العقوبات والقوانين المكملة باستخدام الشبكة المعلوماتية أو أي نظام معلوماتي أو اشترك في ارتكابها بالعقوبة المنصوص عليها في ذلك القانون)).
حيث أشارت هذه المادة إلى الإحالة إلى قانون العقوبات في الجرائم التي لم يرد فيها نص وقد وردت بشأنها عقوبة في قانون العقوبات؛ الأمر الذي ينصرف معناه إلى تطبيق نص المادة (461) المتعلقة بجريمة النصب فيما يتعلق بجرائم الاحتيال الالكتروني.

في حين نرى أنه كان الأولى بالمشرع النص على جريمة الاحتيال الالكتروني في قانون الجرائم الالكترونية؛ نظرًا لما يحمله هذا النوع من الجرائم من خصوصية سواء من ناحية ارتكابها أو من الطرق المستخدمة في ارتكابها.

وعلى صعيد آخر برز نوع آخر من الجرائم الذي تستخدم فيه تقنية التزييف العميق وهي جرائم التزوير باستخدام تقنية التزييف العميق، حيث تساعد هذه التقنية المزورين على تقليد الوثائق والهويات الشخصية، وقد شهدت ليبيا ارتفاعًا في حالات التزييف العميق المرتبط بعمليات الاحتيال في مجال وثائق الهوية بين عام 2020 إلى 2023، حيث بلغت النسبة 100 %(2023,Sumsub Identity Fraud Report) ، مما ينذر بخطر هذه التقنية على الوثائق الرسمية خاصةً في ظل توجه الدولة نحو التحول الرقمي في أغلب القطاعات، وعند الاطلاع على قانون الجرائم الالكترونية نجده لم ينص على جريمة التزوير الالكتروني وبالأخص المتعلق بالوثائق الرسمية كجواز السفر أو البطاقة الشخصية، في حين نجد أن المشرع وفي ذات القانون قد خصص نصوصًا تتعلق بتجريم تقليد الأعمال الرقمية والبرامج التقنية في نص المادة 25 وأيضًا من المادة 28 المتعلقة بتقليد البطاقة المصرفية الالكترونية واستعمالها في حين أهمل النص على تجريم تزوير الوثائق والمستندات الرسمية باستعمال وسائل الكترونية .

الفرع الثاني: التمييز بين التزييف العميق والتزييف الالكتروني العادي

يُمثل التمييز بين جريمتي التزييف العميق والتزييف الالكتروني العادي مسألةً قانونيةً دقيقةً، تؤثر بشكلٍ مُباشر على العقوبة والإثبات والتكييف القانوني، وهذه الأهمية مُستمدة من ضرورة قانونية تفرضها حداثة التقنية، ونعرض لأهم أوجه الشبه في البد أولًا، ثم نعرج على أهم أوجه الاختلاف بينهما في البند ثانيًا، والتي تُميز كل واحدة عن الأخرى استنادًا إلى اعتبارات الخصوصية

أولاً: أوجه الشبه بين الجريمتين :

1. تتطلبُ جرائم التزييف العميق وجرائم التزييف الالكتروني العادي- وجود وسائط الكترونية أو مدخلات يتم عليها التعديل مثل الصور والأصوات والفيديوهات
2. كلتا الجريمتين تتم عن طريق أجهزة الكترونية سواء أكانت حواسيب أو هواتف ذكية أو غيرهم.
3. كلتا الجريمتين يتم التلاعب فيها بالمدخلات سواء كان ذلك بالإضافة أو الحذف والتبديل أو الاستنساخ.

ثانياً أوجه الاختلاف بين الجريمتين :

1. تختلف كلتا الجريمتين من حيث التقنية المستخدمة، ففي التزييف الالكتروني العادي (التزييف السطحي) تستخدم تقنيات بسيطة وغير معقدة مثل برامج تحرير الصور التقليدية والتي يقتصر دورها على مهمات

محدودة كإزالة اللقطات أو النسخ أو اللصق أو قص الصور، بينما تعتمد جرائم التزييف العميق على تقنية التعلم الآلي المبنية على الذكاء الاصطناعي، حيث تستطيع إنتاج مخرجات أكثر واقعية وتنوعًا.

2. يتم التزييف الالكتروني العادي يدويًا؛ مما يؤدي إلى إنشاء تعديلات أقل إقناعًا، على نقيض التزييف العميق الذي يقوم فيه الذكاء الاصطناعي بكل خطوات عملية التعديل، حيث يكون دور العنصر البشري محدودًا فيها .
3. لعل أهم فرق في نظرنا يكمن في كون التزييف الالكتروني العادي أو السطحي يقوم بتشويه السياق بدلاً من تغيير الصور أو الأصوات الفعلية، فهو يقوم على سبيل المثال بتأخير الكلام أو إبطائه أو تغيير الخلفية أو تغيير توقيت الفيديو، ففي أغلب الأحيان يستخدم في تزييف الخطابات السياسية، أما التزييف العميق فهو يقوم بتغيير ملامح الوجه وتعابيره، وكذلك حركات الجسم ويمكنه استبدال الوجوه وتقليد الأصوات بشكلٍ أكثر واقعيةً (OpenGrowth.nd)
4. من السهل اكتشاف التزييف العادي بالمقارنة مع التزييف العميق؛ نظرًا لعدم دقته وعدم تناسق المدخلات المضافة من المحتوى الأصلي.
5. تتطلب جرائم التزييف العادي وقتًا وجهدًا كبيرين إذا ما قورنت بجرائم التزييف العميق؛ ويُعزى ذلك إلى اعتماد هذه الأخيرة بشكل رئيسي على الذكاء الاصطناعي، أما في جرائم التزييف العادي فإن الإنسان هو من يقوم بأغلب عملية التزييف يدويًا.

وخلاصة القول أن جرائم التزييف العميق أشد خطورة من جرائم التزييف العادي، فهي ذات نطاق أوسع ودقة أكبر والتقنية المستخدمة سهلة الاستخدام وغير مكلفة وتعطي نتائج أسرع، فلم يتوقف خطر تقنية التزييف العميق عند مسألة الإضرار بالأفراد أو الشركات فقط، بل طال منظومة العدالة أيضًا، حيث يمكن أن تُستخدم في تضليل المحكمة عن الحقيقة بواسطة اصطناع أدلة غير حقيقية وتقديمها؛ بغية إثبات أو نفي جريمة ما.

المطلب الثاني: التزييف العميق في ضوء مبدأ الشرعية الجنائية ومدى تأثير هذه التقنية على الدليل الرقمي.

حيث سنناقش في هذا المطلب مبدأ تقنية التزييف العميق في ظل مبدأ الشرعية الجنائية، وهل من الضروري النص بشكل صريح على تجريم هذه التقنية ام الاكتفاء بالنصوص الحالية وكذلك سنناقش تأثير هذه التقنية على الدليل الرقمي وكيف يمكن تجنب العبث به.

الفرع الأول: تقنية التزييف العميق في ضوء مبدأ الشرعية الجنائية

نظراً للدور الذي يلعبه التزييف العميق في تضليل الرأي العام والتلاعب بالمعلومات، أصبح يشكل تهديداً كبيراً على الافراد والمؤسسات والدول ويرجع ذلك الي قوة هذه التقنية ومقاربتها للواقع بشكل كبير مما سمح بإلصاق تصريحات أو أفعال بأشخاص لم يقوموا بها في الواقع مما دفع العديد من الدول الي إعادة النظر في اطرها القانونية لمواجهة هذه الظاهرة (موافي، 2026، ص1038) ومن التشريعات التي قدمت نموذجاً قانونياً مواكبا للتطورات المصاحبة في هذا المجال التشريع الإيطالي من خلال المادة 612 مكرر quarter من قانون العقوبات التي أدرجت بموجب مشروع القانون الجديد الخاص بالذكاء الاصطناعي لسنة 2025 وتقوم هذه المادة على تجريم كل من ينشر أو يروج أو يوزع محتوى مزيفاً معالجاً عبر الذكاء الاصطناعي دون رضا الشخص المعني متي كان من شأن ذلك أن يلحق به ضرراً جسيماً أو يحدث خداعاً للغير في صدق المحتوى وبهذا النص يكون المشرع الإيطالي قد وضع اساساً تشريعياً في التجريم والعقاب يسهل على القاضي عملية تكييف النص على جميع السلوكيات التي ترتكب بواسطة تقنية التزييف العميق

أما فيما يتعلق بالمشرع الليبي فإنه لم يصدر قانون خاص ينظم استخدام تقنية التزييف العميق أو حتى تجريم الأفعال المرتكبة بواسطتها، ولكن يوجد بعض المواد ضمن قانون مكافحة الجرائم الالكترونية رقم 5 لسنة 2022 يمكن سريانها على الاستخدام غير المشروع لهذه التقنية مثل جريمة إنتاج المواد الإباحية أو جريمة

مزج أو تركيب الصوت والصور، غير أن هذه النصوص لا تزال عامة ولا تستوعب كل الأفعال والسلوكيات وكذلك الوسائط التي قد ترتكب من خلالها جرائم التزييف العميق ، الامر الذي يرتب نتيجة مهمه وهيا وجود أفعال تمثل اعتداء على مصلحة معينة دون وجود نصوص تستوعبها ما يجعل القاضي الجنائي يقف عندها كونه مقيد بمبدأ الشرعية الجنائية (لا جريمة ولا عقوبة إلا بنص) والذي يجعل القاضي لا يعاقب على فعل لم يجرمه المشرع ولا أن يطبق عقوبة غير منصوص عليها في القانون أو تختلف نوعها أو مقدارها عن تلك المنصوص عليها قانوناً (لخميسي، 2005، ص11)

وطبقاً للقواعد العامة فإن مبدأ الشرعية الجنائية من الناحية الموضوعية يقوم على فكرة التحذير المسبق أي تحذير الافراد من القيام بأفعال معينة توقعهم تحت طائلة العقاب (وزير، 1999، ص33)، وعليه فإن غياب هذه الفكرة عن جرائم التزييف العميق يجعل من غير الممكن العقاب على جرائم التزييف العميق.

لم تتوقف مشكلة جرائم التزييف العميق عند حد التجريم والعقاب، بل أثر هذا النوع الحديث من الجرائم على قواعد المسؤولية الجنائية ايضاً لاسيما فيما يتعلق بتحديد الفاعل الحقيقي للجريمة فغالباً ما تُنتج هذه المحتويات من خلال خوارزميات مفتوحة المصدر، أو تعدل لاحقاً بواسطة أطراف متعددة لا تجمعها علاقة مباشرة، الامر الذي يطرح إشكاليات قانونية متعددة حول:

1- تعدد مستويات المسؤولية (من أنشأ المحتوى؟ من نشرة؟ من حرض عليه؟ من استفاد منه؟

2- صعوبة إثبات الركن المعنوي أو النية الإجرامية في حال الاعتماد على أدوات ذكية تعمل تلقائياً، وقد أكدت اللجنة القانونية للأمم المتحدة المعنية بالجرائم السيبرانية في تقريرها لعام 2023 على "ضرورة تطوير قواعد الاثبات الجنائي لتلائم طبيعة الجرائم الناتجة عن الذكاء الاصطناعي حيث يصعب التحقق من المسؤول الفعلي في سلاسل الإنتاج التقني المعقدة (الشافعي،2025، ص765)

ولكن يمكن حل الإشكالية السابقة وذلك عبر تمكين الشرعية الجنائية من خلال سن نصوص تنظم الأفعال التي ترتكب عبر تقنية التزييف العميق وتحديد السلوكيات التي تمثل اعتداء على حقوق الافراد ووضع عقوبات مناسبة لها، بالإضافة الي تطوير قواعد المسؤولية الجنائية الامر الذي يسهل على القاضي تطبيق النص المطابق للواقعة.

الفرع الثاني: قيمة الدليل الرقمي في ظل تقنية التزييف العميق

تلعب الأدلة الرقمية دورًا مهمًا في عملية الإثبات الجنائي ميدان الجرائم الالكترونية ،ففي كثير من الأحيان يكون الدليل الرقمي هو الشاهد الوحيد على ارتكاب الجريمة؛ نظرًا لطبيعة الجرائم الالكترونية، فهي تنطوي على مسرح جريمة افتراضي وغير مادي، ويعتبر الدليل الرقمي كالدليل العادي من ناحية إمكانية التلاعب به و تغييره والعبث به، ولعل أهم التقنيات التي يمكن أن تستخدم في ذلك هي تقنية التزييف العميق، وسوف نقف في هذا الفرع على ماهية الدليل الرقمي وكيفية تأثير تقنية التزييف العميق وحجيته في ظل وجود هذه التقنية، وما السبيل إلي وجود دليل رقمي سليم أمام المحكمة.

أولاً: مفهوم الدليل الرقمي وتأثير تقنية التزييف العميق عليه

نحاول في هذا المقام جاهدين تسليط الضوء على مُصطلح الدليل الرقمي سواءٌ من حيث تعريفه في البند أولًا، ومن حيث تأثيره في جريمة التزييف العميق وتأثره بها في البند ثانيًا، ولا يعني الإتيان بهذا الضبط الاصطلاحي في القانون رقم 2022/5 بشأن مكافحة الجرائم الالكترونية، إنكار محاولات البعض وجهودهم

1: تعريف الدليل الرقمي عُرف الدليل الرقمي في المادة (1) الفقرة (7) من القانون رقم 5 لسنة 2022م بشأن مكافحة الجرائم الالكترونية بنصه على انه نتائج تحليل البيانات من أنظمة الحاسوب أو شبكات الاتصال أو أجهزة التخزين الرقمية بمختلف أنواعها (المادة 1 من القانون رقم 5 لسنة 2022 بشأن الجرائم الالكترونية)

ويعرف أيضًا بكونه الدليل المأخوذ من أجهزة الكمبيوتر وهو يكون في شكل مجالات أو نبضات مغناطيسية أو كهربائية يمكن تجميعها وتحليلها باستخدام برامج وتطبيقات وتكنولوجيا وهي مكون رقمي لتقديم معلومات

في أشكال متنوعة مثل النصوص المكتوبة أو الصور أو الأصوات أو الأشكال والرسوم ..... (عبد المطلب، ممدوح عبد الحميد، 2006)

ومما سبق نستنتج أن الدليل الرقمي هو مجموعة من البيانات الرقمية المثبتة لواقعة إجرامية حصلت في الفضاء الافتراضي وتم استخراجها من الأجهزة الالكترونية أو الشبكة الدولية، وقد يكون في صورة نهائية أو يحتاج إلى تحليل من قبل متخصصين ومنها الصور والفيديوهات والتسجيل الصوتي والبصمة الرقمية وغيرها.

2: تأثير تقنية التزييف العميق على الدليل الرقمي

لا يقتصر خطر جريمة التزييف العميق على ارتفاع نسبة استخدامها في ارتكاب جرائم كالتشهير أو الابتزاز أو التزوير فحسب، بل قد تستخدم هذه التقنية لتضليل العدالة وإرباكها؛ وذلك عبر العبث بالأدلة المُزمع تقديمها أمام المحكمة والتزييف أمام القضاء يأخذ صورتين:

الصورة الأولى: الدفاع السلبي ويكون من خلال الادعاء أمام القضاء بعدم مصداقية الأدلة المقدمة من فيديو أو صورة أو تسجيل صوتي والادعاء بأنها من صنع التزييف العميق وهي ظاهرة خطيرة تزعزع الأدلة الجنائية أمام القضاء.

الصورة الثانية: فهي التزييف الإيجابي حيث يقوم المتهم بتقديم دليل هو عبارة عن محتوى رقمي مزيف يظهره في مكان آخر بعيد من مكان ووقت الجريمة (مغايرة، 2024، ص142)

وعند الرجوع إلى القانون رقم 5 لسنة 2022 م بشأن الجرائم الالكترونية نجده قد خصص مادة متعلقة بإتلاف الأدلة القضائية الرقمية وتحديدًا في نص المادة 36، حيث نص على أنه يعاقب بالسجن...كل من قام بإتلاف أدلة قضائية معلوماتية أو بإخفائها أو التعديل فيها أو محوها أو العبث بها بأي شكل من الأشكال (المادة 36 من القانون رقم 5 لسنة 2022 بشأن الجرائم الالكترونية)

حيث نلاحظ أن المشرع قد جرم جميع أشكال التلاعب بالأدلة الرقمية أو العبث بها، لكن نجد أن هذه المادة قد أغفلت النص على تجريم سلوك آخر يؤثر على عملية الإثبات أي مسألة إنشاء أو اختلاق دليل، وهو قيام الجاني بإنشاء دليل عبر تقنية التزييف العميق؛ نافيًا عن نفسه

الاتهام أو ناسبًا إياه إلى غيره، ويختلف هذا السلوك عما جاءت به المادة 36 في كونها قائمة على افتراض وجود دليل صحيح مُرتبط بالواقعة ولكن تم التلاعب به بشكل معين، في حين أن اختلاق الدليل قائم على إنشاء دليل وهمي وغير صحيح بالكامل ومن صنع الجاني، يهدفُ من ورائه إلى التشويش على المحكمة وإبعادها عن الحقيقة.

وتأسيسًا على ذلك يمكن القول بأن الدليل الرقمي في ظل وجود تقنية التزييف العميق يجب أن يخضع لمجموعة من المراحل من التدقيق والتقييم لمعرفة مدى سلامته من التغيير أو التعديل ويكون ذلك بمعرفة متخصصين، وفي الفرع الثاني نتعرف على أهم الخطوات المطلوبة للتأكد من سلامة أي دليل رقمي من التعديل أو العبث قبل عرضه على المحكمة.

الفرع الثاني: إجراءات قبول الدليل الرقمي

تُمكن الطبيعة الفنية الخاصة بالدليل الرقمي من العبث بمضمونه على نحو يحرف الحقيقة

دون أن يكون المتخصص قادرًا على إدراك ذلك العبث، فضلًا عن ذلك فإن نسبة الخطأ في إجراءات الحصول على دليل صادق في الإخبار عن الحقيقة تبدو عالية في مثل هذا النوع من الأدلة، ويضاف على ذلك ظهور أدوات تساعد على العبث بالدليل الرقمي وكذلك إنشاء هذا الدليل قبل حتى وقوع الجريمة كأدوات التزييف العميق وفيما يلي بعض الإجراءات التي يمكن اتخاذها لضمان صحة الدليل وأنه مرتبط بالواقعة ويمكن التعويل عليه في إثبات أو نفي الواقعة الإجرامية، ومن هذه الإجراءات

1. الإشارات البيولوجية: حيث تستند هذه التقنية في اكتشاف التزييف العميق عبر ملاحظة العيوب في التغيرات الطبيعية في لون البشرة والتي تنشأ عن تدفق الدم عبر الوجه (Javahir Askari,2023)

2. تحليل الوجوه والحركات: ويكون ذلك عبر التركيز على الوجه عند الحركة وملاحظة وجود عيوب مثل عدم وضوح الرؤية أو وميض حول حافة الوجه قد تبدو الأذنان أيضًا بلون بشرة مختلف تمامًا عن لون الوجه.
3. I lluminarty :حيث تتيح هذه الأداة القدرة على كشف الصور والنصوص المولدة بالذكاء الاصطناعي، وتتضمن النسخة المجانية خدمات أساسية، كما يمكن للمستخدم عن طريق هذه الأداة تحديد مكان التلاعب في الصورة المزيفة وأي نموذج للذكاء الاصطناعي بواسطته تم توليدها، كما يمكنها أيضًا تقييم مدى احتمالية توليد صورة بالذكاء الاصطناعي من عدمه (ايمانويل سالاكو، 2023).
4. استخدام أنظمة كشف قائمة على الذكاء الاصطناعي: حيث يتم استخدام أدوات الذكاء الاصطناعي للكشف عن أي خلل كعدم تناسق البيكسل وحركات الوجه غير الطبيعية وعدم انتظام الرمش أو عدم تطابق الظلال (Shaurya Rawal،2024)، وميزة هذه الأدوات أنها تستخدم نفس التقنية التي يتم بها إنشاء المحتوى المزيف، لذلك في الغالب تكون نتائجها دقيقة وسريعة.

الخاتمة

تعد تقنية التزييف العميق والجرائم المتولدة عنها ظاهرةً حديثةً في ليبيا نتجت عنها آثار سلبية خطيرة تمس الأمن والاستقرار الاجتماعي، حيث دفعت سهولة استخدامها وسرعة الوصول إليها وانخفاض تكلفتها إلى جعلها أداة في مُتناول أي شخص، ومن خلال هذا البحث نخلص إلى النتائج والتوصيات الآتية :

أولاً النتائج :

1. التزييف العميق هو العملية التي يتم فيها تغيير الصور والفيديوهات والأصوات بشكل يخالف حقيقتها؛ بقصد الإضرار بالغير أو الحصول على نفع.
2. تعتمد تقنية التزييف العميق أساسًا على الذكاء الاصطناعي، وهذا هو محور خطورتها.
3. قصور قانون الجرائم الالكترونية الليبي على استيعاب أنماط الجرائم التي ترتكب بواسطة التزييف العميق.
4. عدم نص المشرع الليبي على جريمة الابتزاز الالكتروني، رغم أنها من بين الجرائم الشائعة والمنتشرة بشكل كبير .
5. إن ما يميز التزييف العميق عن التزييف العادي هو أن الأول يستخدم الذكاء الاصطناعي، بينما يستخدم التزييف العادي أدوات تحرير بسيطة.
6. يمكن للتزييف العميق أن يؤثر على عملية الإثبات الجنائي، وذلك لكونه قادر على صنع أدلة واقعية بكل سهولة وفي وقت قصير.

ثانياً التوصيات:

1. نوصي المشرع الليبي بإعداد قانون يتعلق بالجرائم التي ترتكب بواسطة الذكاء الاصطناعي والتي تندرجُ تحتها جرائم التزييف العميق.
2. وضع مجموعة من الشروط والإجراءات قبل قبول أي دليل رقمي أمام المحكمة للتأكد من عدم العبث به أو تغييره .
3. توعية وتثقيف المجتمع حول مخاطر التزييف العميق عن طريق الندوات والمؤتمرات العلمية.

قائمة المراجع

أولا: الكتب:

1- عبد المطلب، ممدوح عبد الحميد، 2006، البحث والتحقيق الجنائي الرقمي في جرائم الكمبيوتر والإنترنت دار الكتب القانونية، مصر.
2- وزير، عبد العظيم مرسي، 1999، شرح قانون العقوبات القسم العام، دار النهضة العربية.

ثانياً: المجلات العلمية:

1- إبراهيم البيومي، رضا، الحماية القانونية من مخاطر تطبيقات التزييف العميق في الفقه الإسلامي والقانون الوضعي دراسة تحليلية مقارنة، مجلة روح القوانين، عدد خاص بالمؤتمر العلمي الدولي الثامن التكنولوجيا والقانون.
2-البرنامج الوطني للذكاء الاصطناعي، دليل التزييف العميق، يوليو 2021، الإمارات العربية المتحدة.
3- الشافعي، عماد الدين حامد،2025، المواجهة الجنائية عن استخدام تقنيات التزييف العميق دراسة مقارنة، المجلة القانونية الاقتصادية، المجلد37، العدد54.
4 - الهيئة السعودية للبيانات والذكاء الاصطناعي، مبادئ التزييف العميق، النسخة (1)
5- لخميسي، عثمانية، 2005، التفسير في المادة الجزائية وأثره على حركة التشريع، مجلة العلوم الإنسانية جامعة محمد خيضر بسكره، العدد السابع.
6-محرم، أحمد مصطفى، 2022، استخدام الذكاء الاصطناعي (AI) استخدام التزييف العميق (Deepfake) في قذف الغير نموذجًا (دراسة فقهية مقارنة معاصرة)، مجلة البحوث الفقهية والقانونية، العدد 39.
7- مغايرة، علاء الدين منصور، 2024، جرائم الذكاء الاصطناعي وسبل مواجهتها: جرائم التزييف العميق نموذجاً، المجلة الدولية للقانون، جامعة قطر، المجلد الثلث عشر، العدد المنتظم الثاني.

ثالثاً: القوانين:

1- القانون رقم 5 لسنة 2022 بشأن مكافحة الجرائم الالكترونية
2- قانون العقوبات الليبي

رابعاً: المراجع الالكترونية العربية:

1ــ ايما نويل سالاكو، أدوات الذكاء الاصطناعي لمكافحة التزييف العميق، 2023.9.27 تاريخ الزيارة 2025.3.20 https;//ijnet.org
2- التزييف العميق (Deepfake) في التصيد الالكتروني: التحديات والحلول، 19/ 12/ 2024، www.cerebra.com
3- خرواط، محمد عبد اللطيف، (17 ديسمبر 2024)، التزييف العميق والاحتيال الصحي: استغلال الثقة بالأطباء لتضليل المرضى والترويج لمنتجات غير موثوقة، تم الاطلاع عليه في 18 فبراير 2025 الساعة 10:30م، (نسخة الكرتونية)، الرابط: https//www.misbar.com

خامساً: المواقع الالكترونية الأجنبية:

1-Deepfakes vs shallow fakes understanding the layers of Digital Deception موقع الكتروني http://OpenGrowth.com
2- https:\\www.awarc.com/blog-how-does deep fake-technology-work- تاريخ2 الزيارة\2\2025 الساعة 5:52م
3-Javahir Askari,18 Aug 2023, Deepfakes and synthetic Media: what are they and how are techuk members taking steps to tackle misinformation and fraud last visited march 20,2025), https: www.techuk.org
4-Shaurya Rawal, deepfakes: comprehensive Analysis, challenges, Mitigation, and foremsic Investigation,11.9.2024, (last visited 22.3.2025) ,http;//www.linkedin.com.
5-Sumsyb Research: Global Deepfake lneldents surge Tenfold from2022to2023 الموقع الالكتروني https:\\sumsub.com

References

First: Books:

1. Abdel-Muttalib, Mamdouh Abdel-Hamid, 2006, Digital Criminal Investigation and Research in Computer and Internet Crimes, Dar Al-Kutub Al-Qanuniyya, Egypt.
2. Wazir, Abdel-Azim Morsi, 1999, Explanation of the Penal Code, General Section, Dar Al-Nahda Al-Arabiya.

Second: Scientific Journals:

1. Ibrahim Al-Bayoumi, Reda, Legal Protection from the Dangers of Deepfakes in Islamic Jurisprudence and Positive Law: A Comparative Analytical Study, Ruh Al-Qawanin Journal, Special Issue for the Eighth International Scientific Conference on Technology and Law.
2. National Artificial Intelligence Program, Deepfakes Guide, July 2021, United Arab Emirates.
3. Dr.Hala mohamed imam mohamed. (2024). Legal challenges in the use of artificial intelligence techniques in editing and refereeing scientific research. Al-Haq Journal for Sharia and Legal Sciences, 86-109. https://doi.org/10.58916/alhaq.vi.238

4. Al-Shafi'i, Imad El-Din Hamed, 2025, Criminal Confrontation of the Use of Deepfakes: A Comparative Study, Al-Qanuni Al-Iqtisadiyya Journal, Volume 37, Issue 54. 4. Saudi Authority for Data and Artificial Intelligence, Principles of Deepfakes, Version (1)
5. Lakhmissi, Othmania, 2005, Interpretation in Criminal Law and its Impact on Legislation, Journal of Humanities, Mohamed Khider University of Biskra, Issue 7.
6. Khalleefah, A. B., Abdalqadir, M. A., & Salem, A. A. (2025). Towards a New Theory of Civil Liability in the Context of Artificial Intelligence Systems and the Challenges of Reforming the Traditional Theory. Al-haq Journal for Sharia and Legal Sciences, 754-770.
7. Muharram, Ahmed Mustafa, 2022, The Use of Artificial Intelligence (AI): The Use of Deepfakes in Defamation as a Case Study (A Contemporary Comparative Jurisprudential Study), Journal of Jurisprudential and Legal Research, Issue 39.
8. Maghayra, Alaa El-Din Mansour, 2024, Artificial Intelligence Crimes and Ways to Combat Them: Deepfakes as a Case Study, International Journal of Law, Qatar University, Volume 13, Regular Issue 2.

Third: Laws:

1. Law No. 5 of 2022 on Combating Cybercrimes
2. Libyan Penal Code Fourth: Arabic Electronic Resources:
3. Emma Noel Salako, Artificial Intelligence Tools to Combat Deepfakes, September 27, 2023 (accessed March 20, 2025) https://ijnet.org
4. Deepfakes in Phishing: Challenges and Solutions, December 19, 2024, www.cerebra.com
5. Kharwat, Mohamed Abdel Latif, December 17, 2024, Deepfakes and Health Fraud: Exploiting Trust in Doctors to Mislead Patients and Promote Unreliable Products (accessed February 18, 2025 at 10:30 PM, hard copy), https://www.misbar.com

Fifth: Foreign Websites:

1. Deepfakes vs. Shallow Fake: Understanding the Layers of Digital Deception (website) http://OpenGrowth.com –
2. 2https:\www.awarc.com/blog-how-does deep fake-technology-work- Date2 Visit\2\2025 at 5:52 PM
3. 3-Javahir Askari, 18 Aug 2023, Deepfakes and synthetic Media: what they are and how are techuk members taking steps to tackle misinformation and fraud last visited March 20, 2025), https: www.techuk.org
4. 4-Shaurya Rawal, deepfakes: comprehensive analysis, challenges, mitigation, and foremsic investigation, 11.9.2024, (last visited 22.3.2025), http;//www.linkedin.com.
5. 5-Sumsyb Research: Global Deepfake lneldents surge tendfold from 2022 to 2023 Website https:\sumsub.com

Disclaimer/Publisher's Note: The statements, opinions, and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of **JLABW** and/or the editor(s). **JLABW** and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions, or products referred to in the content.