73 Original Article Arab Journal for Security Studies 2026; Volume 42 Issue (1), 73-87

Naif Arab University for Security Sciences
Arab Journal for Security Studies
المجلة العربية للدراسات الأمنية
https://journals.nauss.edu.sa/index.php/ajss

AJSS

Legislative Adequacy to Address Crimes Arising From Deepfakes: A Comparative Analytical Study

الكفاية التشريعية لمواجهة الجرائم الناشئة عن التزييف العميق: دراسة تحليلية مقارنة

عمرو أحمد فؤاد
أكاديميَّة الشرطة المصريَّة، جمهورية مصر العربية

Amr Ahmed Fouad
Egyptian Police Academy, Arab Republic of Egypt

Received 16 June 2025; accepted 9 Nov. 2025; available online 19 May 2026

Abstract

Deepfakes have raised numerous legal challenges in recent years. This study aims to assess the adequacy of legislation in the Arab Republic of Egypt and the Kingdom of Saudi Arabia to address crimes arising from deepfakes, in light of relevant European Union regulations, and to identify any legislative gaps created by this technology. The study employs a comparative analytical approach to examine legal texts, highlighting the legal protections afforded to public and private interests, both tangible and digital, against violations that may result from the malicious use of deepfakes. It also explores the powers of investigative authorities to detect fake content and track down perpetrators, as well as the legal obligations of service providers to cooperate with these authorities to achieve justice without violating user privacy. Furthermore, the study reviews the most prominent open-source deepfakes detection tools and evaluates their reliability and admissibility as evidence in criminal cases. The study concluded that the legal frameworks in Egypt and the Kingdom are generally characterized by the protection of interests, without requiring the use of a specific tool or method to infringe upon them. The broad scope of criminalization in both countries is sufficient to punish the end user (the perpetrator). However, these frameworks do not impose controls or obligations on actors

Keywords: *security studies, deepfakes, law, artificial intelligence, digital evidence, digital watermarking*

المستخلص

أثارت تقنية التزييف العميق العديد من التحديات القانونية خلال السنوات السابقة؛ ومن ثمَّ تهدف الدراسة إلى الوصول إلى مدى الكفاية التشريعية بجمهورية مصر العربية والمملكة العربيَّة السعوديَّة لمواجهة الجرائم الناشئة عنها في ضوء لوائح الاتحاد الأوروبي ذات الصلة، وعلى رأسها لائحة الذكاء الاصطناعي؛ للوقوف على الفجوات التشريعيَّة التي سببتها التقنية. واتبعت الدراسة المنهج التحليلي المقارن لتحليل النصوص القانونية، وإبراز الحماية القانونية للمصالح العامة والخاصة، المادية والرقمية، من الانتهاكات التي قد يسببها الاستخدام الخبيث للتقنية، وإظهار صلاحيات جهات التحقيق لكشف المحتوى المزيف، وتتبع الجناة، والالتزامات القانونية الواقعة على مزودي الخدمة للتعاون معها لتحقيق العدالة دون انتهاك لخصوصية المستخدمين. واستعرضت أهم أدوات كشف التزييف العميق مفتوحة المصدر، وعملت على تقييم موثوقيتها وحُجيتها للإثبات الجنائي. وتوصلت إلى اتسام الإطار القانوني بمصر والمملكة العربية السعودية بالعموم في حماية المصالح، دون اشتراط استخدام أداة أو طريقة للاعتداء عليها، واتساع نطاق التجريم بهما، ويكفي ذلك لمعاقبة المستخدم النهائي (الجاني)، لكنه لا يضع ضوابط والتزامات على الأطراف الفاعلة في سلسلة قيمة التزييف

الكلمات المفتاحية: الدراسات الأمنية، التزييف العميق، القانون، الذكاء الاصطناعي، الأدلة الرقمية، العلامة المائية الرقمية

* Corresponding Author: *Amr Ahmed Fouad*
Email: pro.amrfouad@gmail.com

doi: 10.26735/UQHP9428

العميق، ولا يحفزها على الالتزام بمعايير الشفافية، فضلًا عن عدم وجود حماية مباشرة لسلوك ومشاعر الشخص الطبيعي التي أصبح التزييف العميق يُحاكيها بدقة عالية. وأثبتت الدراسة حُجية العلامة المائية الرقمية غير المرئية في الإثبات. وأوصت بدفع مزودي الخدمة بتضمينها في المحتوى المزيف، وتوفير أدوات موثوقة لتمكين جهات التحقيق من الكشف عنها وتحديد المصدر، وقد اعتمدت الدراسة على المنهجين الوصفي التحليلي والمقارن.

in the deepfake value chain, nor do they incentivize them to adhere to transparency standards. Furthermore, there is no direct protection for the behavior and feelings of ordinary individuals, which deepfakes now mimic with high accuracy. The study also demonstrated the evidentiary value of invisible digital watermarks. It recommended that service providers be required to include watermarks in fake content and that reliable tools be provided to enable investigators to detect and identify the source of these watermarks, The study relied on the descriptive analytical and comparative methods.

1. المقدمة

يشهد العالم ثورة تقنية غير مسبوقة تستدعي الإسراع في مواكبتها، بيد أن التحدي الحقيقي يتمثل في المُضي قدمًا دون إغفال ما ينجم عن التطور من تهديدات. وقد برهن التزييف العميق على أن التطور التقني أثمر مكاسب، وأفرز تحديات في آنٍ واحد. فعلى الرغم من تحقيق الاستخدام الطبيعي له لمنافع اجتماعية واقتصادية، فإن الاستخدام الخبيث قد يسبب أضرارًا تتعدى الحدود. وتزداد الخطورة كلما زادت دقة أدواته، وسرعة انتشارها، وسهولة استخدامها، حتى أصبح من الصعب التحقق من زيف المحتوى. ولا شك في أن ذلك يثير حزمة من التحديات القانونية، وبات للجرائم أنماط جديدة يصعب إثباتها بالأدلة التقليدية، وانتقل مسرحها من البيئة المادية إلى الإلكترونية. وصار لزامًا إعادة النظر في مدى كفاية التشريعات الوطنية القائمة لمواجهة هذا النوع من الجرائم، من حيث التجريم أو الإثبات أو تتبع الجناة. وتتناول الدراسة بالتحليل والمقارنة مدى كفاية التشريعات بجمهورية مصر العربية والمملكة العربية السعودية لمواجهة الجرائم الناشئة عن التزييف العميق في ضوء لوائح الاتحاد الأوروبي ذات الصلة، وعلى رأسها لائحة الذكاء الاصطناعي.

مشكلة الدراسة

لا مناص من الاعتراف بأن تطور التزييف العميق غير المسبوق ودقته العالية في محاكاة شكل وسلوك ومشاعر البشر قد تسببا في ظهور أنماط مُستحدثة للجريمة. وقد فرض ذلك ثلاث إشكاليات واضحة تتناولها الدراسة، وهي:

- نطاق تجريم الاستخدام الخبيث للتقنية.
- الإثبات الجنائي في البيئة التقنية المُعقدة.
- تحديد الجناة ومصدر المحتوى المزيف.

وبسبب اختلاف الأنظمة القانونية القائمة في مصر والمملكة العربية السعودية والاتحاد الأوروبي، توسعت الدراسة في نطاق البحث عن كفاية النصوص القانونية بالتشريعات المختلفة بهما لتحديد الإطار القانوني الكامل للمواجهة. وطرحت سؤالين رئيسين، هما: هل التشريعات الحاليَّة بمصر والمملكة العربية السعودية كافية للتصدي للجرائم الناشئة عن التزييف العميق؟ وإن لم تكن كافية، فما الذي تحتاج إليه لكفايتها؟

وانبثق منهما عدد من التساؤلات الفرعية، منها:

- ما نطاق تجريم التزييف العميق في التشريعات المصرية والسعودية؟
- كيف تعامل قانون الاتحاد الأوروبي مع التزييف العميق؟
- كيف يمكن كشف المحتوى المزيف؟ وهل تتمتع الأدوات المستخدمة في الكشف بموثوقية كافية؟ وما الموقف التقني للعلامة المائية الرقمية غير المرئية؟ وما حجيتها في الإثبات؟
- ما صلاحيات جهات التحقيق لملاحقة الجناة؟ وما التزامات مزودي الخدمة؟
- ما حجم التعاون الدولي للتصدي للتحديات الناشئة؟

أهداف الدراسة

1. الوقوف على مدى الكفاية التشريعية بمصر والمملكة العربية السعودية لمواجهة الجرائم الناشئة عن التزييف العميق، وتحديد الفجوات التي تعوق مكافحة هذا النوع من الجرائم إن وجدت.
2. الاستفادة من التجارب المقارنة، وخصوصًا الاتحاد الأوروبي.
3. استعراض وتقييم أبرز الأدوات المستخدمة في كشف التزييف العميق، والوصول للأدوات الموثوقة والصالحة إجرائيًّا.
4. تسليط الضوء على حُجية الأدلة الرقمية في الجرائم الناشئة عن التزييف العميق تقنيًّا وإجرائيًّا.
5. الوصول إلى الدعم القانوني الذي منحه المشرع السعودي والمصري لجهات التحقيق، والالتزامات القانونية لمزودي الخدمة.
6. إظهار الجهد الدولي المبذول لوضع آليات وضوابط قانونية مشتركة لإثبات زيف المحتوى وتتبع الجناة.

أهمية الدراسة

يُعدُّ موضوع التزييف العميق أحد أهم الموضوعات المطروحة على الساحة البحثية القانونية العربية والعالمية؛ إذ يمس الثقة في الذكاء الاصطناعي، ويحتاج إلى ضوابط لتنظيمه، وينبغي قبل النداء إلى سن تشريعات جديدة في المطلق أن نبحث عن كفاية التشريعات الحاليَّة لمواجهة الجرائم الناشئة عنه.

وللدراسة أهمية من الناحية العلمية؛ حيث تسعى إلى الوقوف على الفجوات التشريعية التي سببها التطور التقني للتزييف العميق، وحجية الأدلة الرقمية في الجرائم الناشئة عنها، وتُسلط الضوء على الضوابط الإجرائية لاستخدام جهات التحقيق لآليات الإثبات وتتبع الجناة. وتستعرض التزامات مزودي الخدمة بالتعاون لتحقيق العدالة والحفاظ على الخصوصية.

ومن الناحية العملية، تركز الدراسة على العقبات التي تواجه جهات التحقيق لإثبات جرائم التزييف العميق، وتُقيم الأدوات المُستخدمة للتحقق من زيف المحتوى، وتطرح العلامة المائية الرقمية غير المرئية كأداة تقنية فعَّالة لكشف التزييف، وتتبع الجناة، وتستكشف الضوابط القانونية والمعايير التقنية لحجيتها في الإثبات.

الدراسات السابقة

دراسة بعنوان: الأدلة الرقمية المتحصلة من التفتيش الجنائي الإلكتروني: دراسة مقارنة (مرعي، ٢٠٢٢). وقد استندت دراستنا إلى ما خلصت إليه الدراسة من قصور قواعد التفتيش التقليدية لاستيعاب الجرائم التقنية، ولا سيما فيما يتعلق بتفتيش البرامج، ونسب الدليل إلى متهم محدد، خصوصًا إن تعمد إخفاء هُويته عبر تدابير فنية.

ثم بروتوكول بيركلي (٢٠٢٤) بشأن التحقيقات الرقمية مفتوحة المصدر، وهو دليل عملي صادر باسم مفوضية الأمم المتحدة لحقوق الإنسان، ومركز حقوق الإنسان في كلية الحقوق بجامعة كاليفورنيا، لاستخدام المعلومات الرقمية في التحقيقات الخاصة بانتهاكات القانون الجنائي الدولي والقانون الدولي لحقوق الإنسان والقانون الدولي الإنساني. واستعرض التقرير الأدوات مفتوحة المصدر المستخدمة، واعتمدت عليه دراستنا عند تقييم الأدوات التي تناسب كشف التزييف.

منهج الدراسة

الدراسة من النوع القانوني النظري غير الكمي، التي تهدف إلى تحديد كفاية التشريعات المصرية والسعودية لاستيعاب تهديدات الاستخدام الخبيث للتزييف العميق في ضوء لوائح الاتحاد الأوروبي؛ ومن ثم تم اختيار المنهج التحليلي المقارن لتحليل النصوص القانونية ومقارنتها. كما استخدمت المنهج الوصفي التحليلي لدراسة الإطار التقني، وآليات التحقق وتقييم موثوقيتها، لتحديد أوجه القصور التقنية والتشريعية، ولمراجعة البيانات الواردة بالتقارير ذات الصلة.

2. المنظور القانوني للجرائم الناشئة عن التزييف العميق

ويتناول التعريفات والخصائص، وآليات التحقق، والبناء القانوني للجرائم الناشئة، ويحدد متى تقع الجريمة، وحجية الدليل الرقمي.

2. 1. ماهية التزييف العميق

يستعرض المفاهيم التقنية والقانونية للتزييف العميق وخصائصه.

2. 1. 1. تعريف التزييف العميق

يُطلق مصطلح التزييف العميق Deepfake على عملية إنتاج محتوى مزيف بصري أو صوتي، يظهر فيه الشخص بمواصفاته الشكلية والسلوكية والصوتية (Altuncu, Franqueira, & Li, ٢٠٢٢).

وينقسم المصطلح إلى كلمة «تزييف» وتعني تزوير وتقليد (معجم المعاني)، و«عميق» التي تدل على الثبات والعُمق (Cambridge Dictionary-).

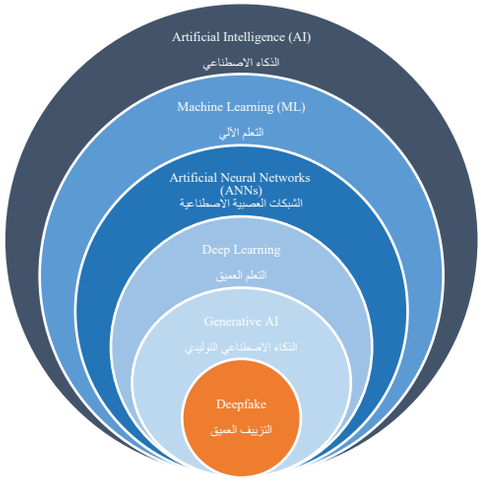
وعرف البعض التزييف العميق بأنه تقنية تُستخدم لإنشاء محتوى مزيف؛ مثل: الفيديوهات أو الصور التي تُظهر أشخاصًا وأحداثًا وأصواتًا وتعابير وجوه مصطنعة، يصعب تمييزها عن الحقيقية (أبو العلا، 2024).

ويشير المصطلح تقنيًا إلى استخدام خوارزميات التعلم العميق Deep Learning التي تُعدُّ فرعًا من فروع الذكاء الاصطناعي، يعتمد على تحليل البيانات باستخدام أكواد برمجية يطلق عليها خوارزميات، لإنتاج مخرجات دقيقة (النجار، 2024).

وقد تطورت الخوارزميات، وأصبحت قادرة على التعلم ذاتيًّا، دون تدخل بشري، وأطلق على هذا النوع مصطلح التعلم الآلي Machine Learning-، ثم صُممت شبكات عصبية اصطناعية Neural Artificial Netwrok لمحاكاة دماغ الإنسان، ونتج عنها زيادة عُمق ودقة الخوارزمية في التعلم، وأطلق على هذا النوع مصطلح التعلم العميق Deep Learning (Janiesch., et al., 2021).

وأدَّى ذلك التطور إلى ظهور الذكاء الاصطناعي التوليدي Generative AI-، الذي تُعدُّ تقنية التزييف العميق أحد أنواعه، لكنها

شكل 1
العلاقة بين تقنية التزييف العميق والذكاء الاصطناعي



من إعداد الباحث

تختلف عن باقي الأنواع القائمة على توليد اللغات الطبيعية، والتوليف الصوتي، وتحسين الكتابة، وإنشاء المجسمات والتصميمات، التي تستخدم في إنشاء محتوى إبداعي جديد، بينما يستخدم التزييف العميق لإعادة إنشاء أو محاكاة ملامح وسلوك وأصوات أشخاص حقيقية، يمكن أن يساء إستخدامها بخلاف باقي الأدوات التي تستخدم في تسهيل الأعمال والأغراض البحثية والإبداعية المشروعة (Schneider et al, 2024).

ويوضح شكل 1 العلاقة بين التزييف العميق والذكاء الاصطناعي وفقًا لما سبق بيانه.

وعرفته لائحة الاتحاد الأوروبي للذكاء الاصطناعي رقم 1689/2024 بأنه محتوى لصورة أو صوت أو فيديو تم إنشاؤه أو التلاعب به، ويشبه الأشخاص أو الأشياء أو الأماكن أو الكيانات أو الأحداث الموجودة، ويبدو بشكل زائف على أنه أصلي وحقيقي.

ويندرج التزييف العميق ضمن نطاق المادة الأولى من نظام مكافحة الجرائم المعلوماتية السعودي (1428هـ) التي عرفت برامج الحاسب الآلي بأنها مجموعة التعليمات والبيانات التي تشمل أوامر أو تطبيقات، تعمل على الحاسب، أو عبر شبكاته، بغرض تنفيذ مهمة معينة.

كما عرفت الجريمة المعلوماتية بأنها كل سلوك يخالف أحكام القانون، يتم ارتكابه باستخدام جهاز الحاسب الآلي أو الشبكة المعلوماتية.

وعرفته الهيئة السعودية للبيانات والذكاء الاصطناعي (سدايا) (2022) بأنه مجموعة من الوسائط الاصطناعية تبدو واقعية، لكنها أنشئت من خلال توظيف تطبيقات الذكاء الاصطناعي، وتتعامل مع الصوت أو الفيديو أو أي محتوى رقمي آخر بطرق يصعب تمييزها عن الواقع.

وفي مصر، تناولت المادة (1) من قانون مكافحة جرائم تقنية المعلومات المصري (2018) تعريفات يندرج التزييف العميق ضمنها، منها: تقنية المعلومات، وهي أي أداة يتم استعمالها لغرض تخزين المعلومات أو البيانات أو استرجاعها، أو تنظيمها أو معالجتها أو تطويرها، سواء عملت تلك الأداة بصورة مستقلة أو متصلة بأخرى.

وعرفت البرنامج المعلوماتي بأنه مجموعة من الأوامر والتعليمات يتم تمثيلها باستخدام رموز أو لغات أو إشارات أيًّا كان شكلها، ويمكن استعمالها بالحاسب الآلي لتنفيذ مهمة أو للوصول إلى نتيجة محددة، سواء نُفذت تلك الأوامر والتعليمات بصيغتها الأصلية أو لا، وسواء تم توظيفها بطريقة مباشرة أو لا.

ويتضح لنا مما سبق، أن الاتحاد الأوروبي قد وضع تعريفًا صريحًا للتزييف العميق، بينما بادرت سدايا إلى تعريفه، ويعكس ذلك إدراكها لضرورة المواكبة السريعة. وعلى الرغم من غياب تعريف صريح في التشريعات المصرية والسعودية، فإن التعريفات الواردة بها تتيح للمحكمة مساحة ومرونة كافية لتكييف السلوك المرتكب في ضوئها، كما أنها تتفق مع جوهر استخدامات التزييف العميق.

2. 1. 2. أهم خصائص التزييف العميق

لا يُعدُّ التزييف العميق بطبيعته ضارًّا، فهو يُستخدم في التعليم، والرعاية الصحية، والترفيه، والتسويق، وتحسين الخدمات، ورفع المبيعات، ونشر الثقافة، والعديد من الاستخدامات التي تحقق منافع اقتصادية واجتماعية.

وفرقت سدايا (2022) بين تقنيات التزييف العميق غير الخبيثة والخبيثة، فعرفت الأولى بأنها الوسائط المُنشأة بأدوات الذكاء الاصطناعي لأغراض حميدة، دون نية خداع أو إضرار. ووصفت الخبيثة بأنها الوسائط المُستخدمة لخداع الأفراد أو إيذائهم أو استغلالهم، وقد تُستخدم في نشر الشائعات أو التشهير أو الاحتيال، وتفتقر إلى الشفافية والإفصاح، وتستخدم صور الأشخاص دون تفويض منهم، أو موافقة، ولا تمتثل إلى التشريعات والمبادئ التوجيهية والأخلاقية.

وتأتي تلك المخاطر بسبب الخصائص التي يمتلكها التزييف العميق، ومن أبرزها:

2. 1. 2. 1. قدرة التزييف العميق على محاكاة الواقع

يتميز التزييف العميق بالدقة العالية في التعرف على الخصائص السلوكية والشكلية للبشر، ورصد وتحليل التفاصيل، ومحاكاة مشاعر الشخص، وسلوكياته وتعبيرات وجهه، وانفعالاته وإيماءات رأسه وحركات جسده وصوته (فؤاد، درويش، حسنين، 2025).

وتعتمد في ذلك على تقنيات مختلفة، أبرزها شبكات الخصومة التوليدية Generative Adversarial Netwroks (GANs)، وهي عبارة عن خوارزمتين، تولد الأولى المحتوى عدة مرات، وتُحسن الثانية من الجودة، وتستبعد النسخ الأقل واقعية، ويستمران في التنافس حتى يصلا إلى أعلى درجة ممكنة من الواقعية (زكير،2022).

2. 1. 2. 2. اعتماد التزييف العميق على البيانات الشخصية

يعتمد التزييف العميق على بيانات شخصية حقيقية، يوفرها المُستخدم لإنشاء محتوى مزيف لشخص طبيعي، بطريقة تحاكي الواقع تمامًا، بما فيه من أماكن وملامح وسلوكيات وانفعالات بشرية. وكلما زاد حجم البيانات، زادت دقة المخرجات (أبو العلا، 2024).

ونلاحظ أن قدرة التزييف العميق على محاكاة سلوك ومشاعر البشر دفعت لائحة الاتحاد الأوروبي للذكاء الاصطناعي إلى ضم الخصائص السلوكية للشخص الطبيعي ضمن تعريف البيانات البايومترية Biometric Data التي تتمتع بحماية أعلى، ووضعت ضوابط لأنظمة التعرف على المشاعر-Emotion Recognition Sys tem التي تعمل على تحديد أو استنتاج مشاعر أو نوايا الأشخاص الطبيعيين.

وهو ما لا يشمله التشريع المصري أو السعودي بحماية مباشرة، مع تمتع الصور ومقاطع الفيديوهات والتسجيلات الصوتية بالحماية القانونية، وفقًا لما ورد من تعريف البيانات الشخصية بنص المادة الأولى من نظام حماية البيانات الشخصية السعودي (1443هـ)، والمادة (1) من قانون حماية البيانات الشخصية المصري (2020).

2. 1. 2. 3. سهولة استخدام التزييف العميق وانتشاره

أتيحت تقنية التزييف العميق للجمهور منذ عام 2017، وشهدت نموًا هائلًا منذ ذلك الحين، ويشير تقرير (Sensity, 2024) إلى أن عدد الأدوات المتاحة وصل إلى 13,522 أداة في عام 2024 (2,298 أداة تبديل الوجه ومزامنة شفاه. و10,206 أداة توليد الصور. و1,018 لأدوات توليد واستنساخ الصوت).

2. 1. 2. 4. تعدد صور الاستخدام الإجرامي للتزييف العميق

شاع استخدام التزييف العميق في توليد محتوى منافٍ للآداب، وتعرض بعض المشاهير إلى الاستغلال بسببه (Citron, D. K., & Chesney, R. 2019). بجانب بعض القضايا ذات الصلة؛ مثل: تأييد محكمة النقض بمصر حكم الاستئناف الصادر بإدانة متهم أضاف صورة وجه طليقته على صورة جنسية للانتقام (حكم محكمة النقض، 2013).

ويشمل الاستخدام الخبيث أيضًا استغلال الأطفال والنساء، والابتزاز، وانتحال الهوية، والاحتيال المالي من خلال تقليد الأصوات الموثوقة وخداع الضحايا لتحويل الأموال، أو كشف معلومات مصرفية، أوتفويض المعاملات، ويمكن أن يُستخدم في التجسس على الشركات أو الإضرار بها، من خلال محاكاة الاتصالات التي يجريها المديرون أو سرقة معلومات مهمة (سدايا،2022).

وتمتد التأثيرات إلى المستوى الاقتصادي أو الاجتماعي للدولة، فقد تستخدم في إثارة الفتنة، أو التأثير على الرأي العام ونشر الشائعات (Goldstein, et al., 2023). ويزداد التأثير إذا تم تزييف محتوى لشخصيات عامة(Giovanni S., et al., 2023)، فقد رصدت دراسة Agarwal وآخرين (2019) العديد من مقاطع الفيديو المزيفة التي ظهر بها شخصيات بارزة، مثل: باراك أوباما وهيلاري كلينتون.

وقد يمتد التأثير إلى المستويين الأمني والعسكري، فقد رُصد مقطع فيديو بموقع X (Twitter سابقًا) للرئيس الأوكراني يأمر فيه الجيش بالاستسلام في الحرب الروسية الأوكرانية، وتبين لاحقًا أنه مقطع مزيف، اسُتخدم لإنشائه مقطع حقيقي مصور سلفًا للرئيس، ولا يزال منشئه غير معروف (Strandord, 2023).

وعامة، يصعب حصر الجرائم الناتجة عن التزييف العميق، بسبب التطور السريع في السلوك الإجرامي، ومحاولة توظيفها في مختلف الجرائم.

2. 1. 2. 5. صعوبة تتبع المحتوى المزيف وإثبات الجريمة

كان من السهل اكتشاف المحتوى المزيف بالعين المجردة دون تحقق فني، من خلال العوامل الواضحة؛ مثل: عدم انتظام ملامح الوجه، وتناقضات الإضاءة، وتغيرات لون البشرة، أو عدم تزامن حركة الشفاه مع الصوت. إلا أن التطور المستمر للتقنية رفع من جودة ودقة المخرجات، وأصبحت تُحاكي الواقع؛ مما جعل اكتشافه بالعين المجردة صعبًا (سدايا،2022).

ويواجه اكتشاف الجرائم الإلكترونية عامة عدة تحديات، منها غياب الأثر المادي الملموس، وغياب الشهود في أغلب الحالات، وصعوبة تحديد الجاني، خصوصًا إذا استطاع محو الأدلة الرقمية (مرعي، 2022). وأصبحت الأدلة التقليدية مثل: بصمات الأصابع، لا تناسب هذا النوع من الجرائم (McGEE,S, 2022)، وبرزت فرص جديدة للتحقيقات الجنائية، يستخدم فيها المحققون البيانات الرقمية المرتبطة بالمواقع الجغرافية والحسابات المصرفية وغيرها من المعرفات لتحديد هُوية الجاني وتتبع نشاطه، واستخدامها في دعم الإدانات وإثبات الجريمة (Casey, et al., 2021).

وفرق بروتوكول بيركلي (2024) بين البيانات الرقمية مفتوحة المصدر open-source data ، التي يمكن لأي شخص الوصول إليها دون حاجة إلى تصريح قانوني، والبيانات مغلقة المصدر closed-source data التي تخضع لقيود قانونية للإفصاح عنها.

وفي هذا السياق، حددت المادة (2) من قانون مكافحة جرائم تقنية المعلومات المصري، والمادة (15) من نظام حماية البيانات الشخصية السعودي التزامات مزودي الخدمة أو مراقبي البيانات بالإفصاح عن البيانات لجهات التحقيق لأغراض المصلحة العامة، أو الأمن، أو الامتثال للمتطلبات القضائية، أو عند الضرورة للكشف عن حقائق تتعلق بارتكاب جريمة يعاقب عليها القانون.

ولا يعني ذلك تجاهل سلطات التحقيق للبيانات مفتوحة المصدر، بل تمتلك أهمية بالغة، حيث تحتاج جهات التحقيق إلى جمع سريع للبيانات عبر الإنترنت قبل الانتقال إلى الموقع، فضلًا عن أن سرعة تبادلها يعزز من قدرة السلطات على جمع المعلومات، خصوصًا عند البحث عن محتوى مزيف أو مكرر. ومن أبرز الآليات التقنية لكشف المحتوى المزيف:

1. **الطب الشرعي الرقمي Digital Forensics**

يعتمد على البصمات الرقمية Fingerprinting أو كشف النسخ Copy Detection، من خلال تخزين الصور ومقاطع الفيديو المزيفة في قاعدة بيانات، وتحويلها إلى تمثيل رقمي مشفر يسمى بالتجزئة Hash، ومقارنة التجزئة الجديدة مع المُخزنة، لتحديد ما إذا كان المحتوى أصليًّا، أو نسخة من إصدار موجود سلفًا (Fernandez P.L., et al., 2024). وتطورت الطريقة لتشمل نظام التجزئة العصبية NeuralHash، وهي دالة تجزئة إدراكية، تعمل على تحليل خصائص المحتوى بدلًا من قيم البكسل الدقيقة.

وتُعدُّ تلك العملية معقدة تقنيًّا، وتحتاج إلى قواعد بيانات ضخمة تُحدَّث باستمرار، وقد تولد تجزئات مختلفة عن الأصلية عند تحرير المحتوى Editing أو اقتصاصه Cropping، أو تسريع الملف الصوتي (Fernandez P.L., et al., 2024).

2. **أدوات تحليل الصور ومقاطع الفيديو**

تعتمد على خوارزميات؛ مثل: «المصنف الثنائي» Binary Classifier»، أو «مكبِر الفيديو» «Video Magnifier» لرصد الاختلافات الدقيقة في المحتوى المزيف، مثل: نبض قلب الشخص في المقطع، أو تغيرات لون جلده (Ahmed, et al., 2023).

ونرى أن معظم تلك الأدوات يفتقر إلى الموثوقية، حتى وإن ساعدت عدة مرات في كشف تزييف المحتوى؛ إذ يمكن لأي مبرمج تصميم ونشر أداته الخاصة دون التأكد من فاعليتها، ودون إصدار تحديثات تواكب التطور السريع في التزييف.

3. **البيانات الوصفية MetaData**: تشير إلى المعلومات الأساسية للصورة أو الفيديو، مثل: موقع ووقت وتاريخ التصوير، ونوع الكاميرا، وأي تعديلات أجريت (Riley, J. 2017) . وتستخرج باستخدام أدوات مصممة لقراءة المعلومات، مثل: ExifTool, Metadata2go.

ولا تكشف تلك الأدوات البيانات الوصفية فقط، بل تسمح للمستخدمين بإزالتها أو تعديلها، وقد دفع ذلك بعض الشركات إلى تطوير أنظمة تشفير عالية الجودة للبيانات الوصفية Cryptographic Metadata لخفض احتمالات الإزالة أو التعديل.

وعلى الرغم من توفير البيانات الوصفية لأدلة حاسمة، فإنها ما زالت عُرضة للإزالة أو التلاعب، وقد تُمحى أو تتغير عند إعادة معالجتها باستخدام برامج التحرير، أو عند أخذ لقطة شاشة screenshot من الهواتف المحمولة. كما أن خوارزميات منصات التواصل الاجتماعي؛ مثل: فيسبوك وإنستغرام تقوم بضغط ملف المحتوى عند مشاركته، وتتغير البيانات الوصفية تلقائيًّا بسبب الضغط (Grommlet, P, et al., 2024).

4. **العلامة المائية الرقمية Digital Watermark**

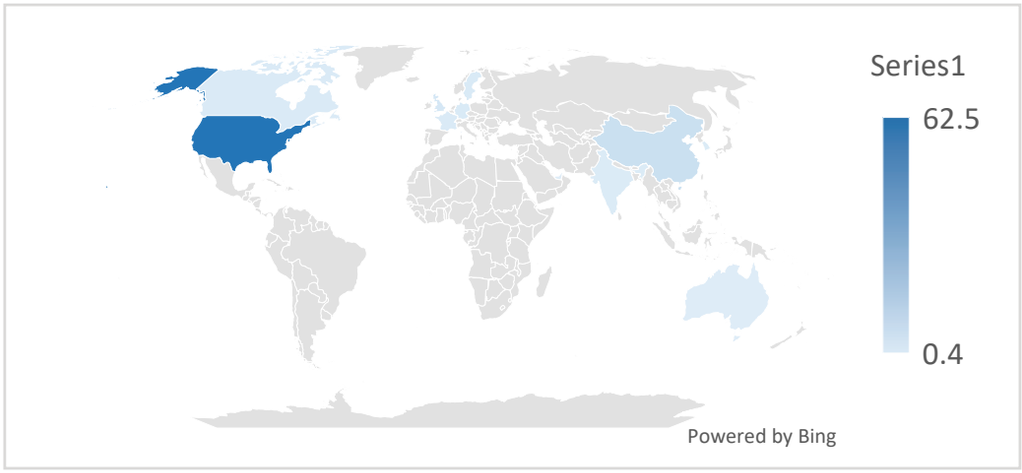
تُعد إضافة فعَّالة لتتبع المصدر، وهي أحد الحلول التكنولوجية الواعدة في مجال التحقيقات الجنائية الرقمية (Wu, X., et al., 2024).

فقد حدد Wadhera وآخرون (2022) السمات التقنية الرئيسة التي تميزها عن التقنيات الأخرى، وخلصت الدراسة إلى أنها تمتلك درجة كبيرة من الأمن والمتانة لتحمل التعديلات والتلاعب، وتتيح التحقق بموثوقية، كما أنها تُخزن كمية كبيرة من المعلومات دون التأثير على الجودة. ويعتبر معرف جوجل Google SynthID من أبرز تطبيقاتها.

وعرف قانون ولاية كاليفورنيا (2024) العلامة المائية الرقمية بأنها المعلومات المُضمنة في مخرجات نظام الذكاء الاصطناعي التوليدي الحاملة لطبيعته الاصطناعية أو هويته أو مصدره أو التعديلات. وألزم مزودي الخدمة بتضمينها في المحتوى، على أن تتمتع بالمتانة والأمن قدر الإمكان، وأن تحتوي على بيانات تُحدد المصدر.

وألزمت لائحة الاتحاد الأوروبي للذكاء الاصطناعي مزودي الخدمة بتضمينها في المحتوى المزيف أيضًا، على أن تكون قابلة للقراءة آليًّا للتحقق من المحتوى.

شكل 2
الاستثمار الخاص في الذكاء الاصطناعي حسب المنطقة الجغرافية في عام 2023، بالمليار يورو



من إعداد الباحث اعتمادًا على بيانات European Parliament, AI Investment: EU and Global Indicators; Statista, (2024 Standord AI Index Report, 2023).

وعلى الرغم من ذلك، نجد أن التشريعات التي دعت إلى تضمين علامة مائية رقمية غير مرئية في المحتوى المزيف ركَّزت على تعزيز شفافية المحتوى المزيف، لكنها لم تُركز على آليات لتمكين جهات التحقيق، ففي حين ألزم قانون كاليفورنيا المزود بتوفير أدوات تحقق مجانية للجمهور، فإنه لم يُلزم بتقديم بيانات عن مصدر المحتوى، وهو أمر طبيعي للحفاظ على خصوصية المستخدمين. ومن ثمَّ، لن يستطيع المحققون خارج كاليفورنيا ملاحقة الجناة. بالإضافة إلى عدم قدرة أداة تحقق وفرها مزود معين على كشف محتوى مزيف مولد من مزود آخر؛ مما يدفع المُحقق إلى تجربة جميع المنصات المفتوحة للتحقق، وهو جهد شاق لا يضمن الوصول إلى نتائج، خصوصًا إن تم توليد المحتوى بدولة لم تُلزم المزود بتضمين العلامة. الأمر الذي يحتاج إلى تعاون على الصعيد الدولي بين الشركات التقنية والحكومات لوضع معايير تقنية وضوابط قانونية للعلامة، تُمكن جهات التحقيق على مستوى العالم، دون المساس بخصوصية المستخدمين.

في جميع الأحوال، تستخدم سلطات التحقيق جميع الأدوات للتحقق وتتبع الجناة، والمُعتد به يخضع لضوابط إجرائية مُحددة.

5. طبيعة التزييف العميق العابرة للحدود

تتسم تقنية التزييف العميق بطبيعة عالمية، حيث يمكن إنتاج المحتوى المزيف في دولة، واستهداف ضحايا في دولة أخرى، وقد تكون الأداة أو الخادم المُستخدم بدولة ثالثة، ويثير ذلك تحديات قانونية تتعلق بالاختصاص القضائي، فضلًا عن صعوبة الوصول إلى بيانات الجناة الرقمية لعدم امتثال المزودين بدولة لقوانين دولة أخرى (مرعي، 2022).

ومن المهم الإشارة إلى أكثر المناطق الجغرافية جذبًا لمزودي الخدمة على مستوى العالم. ولتحديدها، اعتمدت دراستنا على مؤشر الاستثمار في الذكاء الاصطناعي حسب المنطقة الجغرافية. ويوضح شكل 2 حجم الاستثمارات الخاصة في الذكاء الاصطناعي جغرافيًّا في عام 2023 بالمليار يورو.

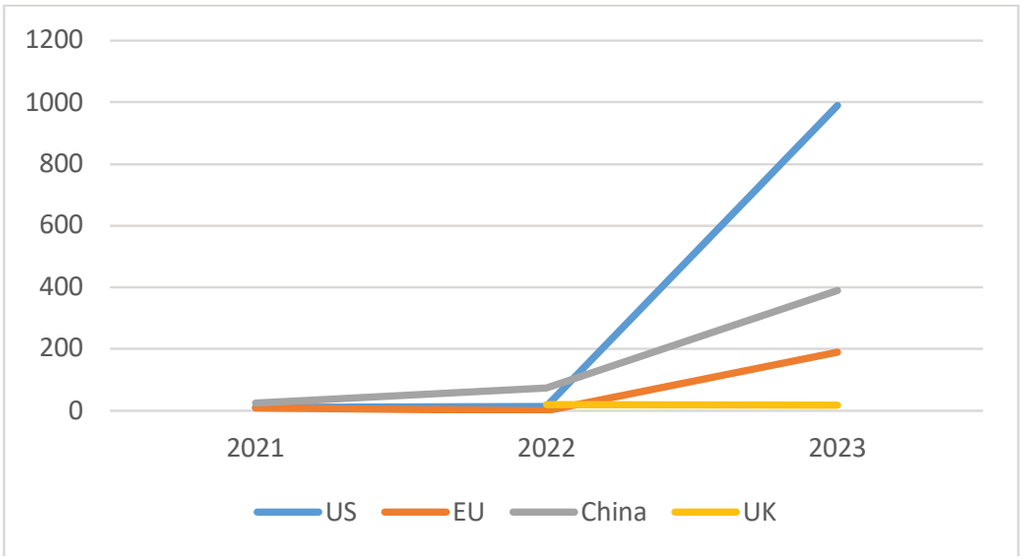
كما يوضح الشكل 2 أن الولايات المتحدة تتصدر قائمة المناطق الأكثر جذبًا للاستثمار الخاص في الذكاء الاصطناعي في عام 2023، بقيمة 62.5 مليار يورو. تليها الصين 73 مليار يورو، والمملكة المتحدة 3.5 مليار يورو، وألمانيا 1.8 مليار يورو، والسويد 1.8 مليار يورو، وفرنسا 1.6 مليار يورو، وكندا 1.5 مليار يورو، وكوريا الجنوبية 1.3 مليار يورو، والهند 1.3 مليار يورو، وسنغافورة مليار يورو، وأخيرًا أستراليا والإمارات العربية المتحدة وإسبانيا 0.4 مليار يورو.

ويوضح شكل 3 حجم استثمار رأس المال في الذكاء الاصطناعي التوليدي الذي يُعدُّ التزييف العميق من أنواعه حسب البلد بين (2021 - 2023) بالمليون يورو.

ويتضح لنا من الشكلين 2 و 3 أن الولايات المتحدة الأمريكية والصين والاتحاد الأوروبي من أكبر الدول والمناطق جذبًا للاستثمار في مجال الذكاء الاصطناعي التوليدي.

ولا شك في أن تلك الريادة تفرض عليها مسئولية دولية نحو وضع أطر قانونية للاستخدام، وتبني سياسات الحوكمة العالمية للتقنية، فلا تؤثر تشريعات تلك الدول على نطاقها الجغرافي فقط، بل يمتد التأثير إلى العالم كله بسبب الطبيعة العابرة للحدود للتقنية.

شكل 3
استثمار رأس المال الاستثماري في الذكاء الاصطناعي التوليدي حسب الدولة/المنطقة، 2021-2023 (بالمليون يورو)



من إعداد الباحث اعتمادًا على بيانات European Parliament, AI Investment: EU and Global Indicators; McKinsey, OECD

6. عدد الأطراف الفاعلة في إنتاج المحتوى المزيف

من المفترض خضوع كافة الأطراف الفاعلة في عملية إنتاج المحتوى المزيف للالتزامات القانونية طوال سلسلة القيمة، وقد تضمنتهم لائحة الاتحاد الأوروبي للذكاء الاصطناعي، ومن أبرزهم المزود Pro-vider الذي يطور النظام، والمُشغل Deployer، وهو مُستخدم النظام، وقد يكون نفسه المزود. والمستورد Importer، إذا كان النظام مستوردًا. كما أنشأ الاتحاد جهات مُخصصة لاعتماد الأنظمة قبل طرحها في السوق، والتأكد من الامتثال لمعايير الشفافية، وأخضعت الأنظمة المطروحة لسلطة مراقبة السوق الأوروبي.

وصنفت اللائحة أنظمة الذكاء الاصطناعي وفقًا لدرجة المخاطر التي قد تنتج عنها، ووضعت التزييف العميق ضمن المخاطر المحدودة Limited Risks التي تحتاج إلى اتخاذ جميع الأطراف لكافة الإجراءات التي تعزز من الشفافية والمصداقية.

بينما عرف نظام حماية البيانات الشخصية السعودي جهة التحكم بأنها المسئولة عن تحديد هدف المعالجة وطريقتها، وأطلق المشرع المصري لفظ المتحكم على هذا الوصف في قانون حماية البيانات الشخصية. وتتفق تلك المفاهيم مع الواردة في اللائحة العامة للبيانات الصادرة عن الاتحاد الأوروبي (GDPR, 2016)، لكنها لا تعبر بدقة عن كافة الأطراف الفاعلة الواردة في لائحة الذكاء الاصطناعي.

ويتضح لنا الحاجة إلى وضع أطر وطنية تُنظم أدوار ومسئوليات الأطراف الفاعلة في إنتاج واستخدام المحتوى المزيف.

2.2. البناء القانوني لجرائم التزييف العميق

2. 2. 1. أركان جريمة التزييف العميق

يُعدُّ الاستخدام الخبيث للتزييف العميق جريمة إذا توافر الركنان المادي والمعنوي، ويؤدي غياب أي ركن إلى زوال النموذج الإجرامي (العجيل، 2021).

2. 2. 1. 1. الركن المادي للجرائم الناشئة عن التزييف العميق

الركن المادي هو السلوك الخارجي المؤثر في الواقع، فلا تُعدُّ الأمنيات والرغبات الداخلية سلوكًا أو جريمة ما دام لم ينتج عنها آثار مادية، تتسبب في الإخلال بالمبادئ أو التعدي على الحقوق. ويتكون من:

- السلوك الذي فعله الجاني.
- النتيجة المتمثلة في الاعتداء على مصلحة عامة أو خاصة، على أن تكون مصلحة محمية بموجب نص قانوني، إعمالًا لمبدأ الشرعية الجنائية بأن لا جريمة ولا عقوبة إلا بنص (القهوجي، 2003).
- علاقة السببية بين السلوك والنتيجة التي تثبت مسئولية الفاعل (حسني، 1983).

2. 2. 1. 2. الركن المعنوي للجرائم الناشئة عن التزييف العميق

هو رغبة الجاني وإرادته المخفية، ويرتكز القصد الجنائي على عنصرين، وينتفي إذا انتفى أحدهما، وهما:

جدول 1

أركان جرائم التزييف العميق

الركن	العنصر	البيان
الركن المادي	السلوك	استعمال برنامج أو تقنية لمعالجة معطيات شخصية للغير.
	النتيجة	ربط المعطيات بمحتوى يُسيء لصاحبها. ونلاحظ أن المشرع اكتفى بتلك النتيجة لوقوع الجريمة، دون أن يشترط التهديد بالمحتوى أو نشره، وتضمنت المادة (6) فقرة (1) من نظام مكافحة جرائم المعلوماتية السعودي نفس النتيجة.
	علاقة السببية	تشكلت بين السلوك والنتيجة، فإذا سبق الفاعل شخص آخر قام بربط معطيات الغير بمحتوى مسيء، فلا تقع مسئولية على الأول لعدم وجود رابط بين الفعل والنتيجة، وتقع على الثاني الذي تحققت النتيجة من جراء فعله.
الركن المعنوي	العلم	عرف الجاني بأنه يستعمل البرنامج لإنشاء محتوى للغير منافٍ للآداب.
	الإرادة	اتجه الجاني عمدًا إلى استعمال البرنامج (السلوك) لمعالجة بيانات الغير لإنشاء محتوى مسيء (النتيجة). وإذا انتفى علمه الذي يفسر إرادته، فبذلك لم يتحقق القصد الجنائي، ويستدل على عدم قصده إذا كان قد أجرى المعالجة لأغراض أخرى غير ربطها بمحتوى منافٍ للآداب، لكنه أخطأ نتيجة إهمال دون رغبة أو قصد.

من إعداد الباحث

- علم الجاني بماهية الفعل.
- إرادته في تحقيق النتيجة من جرائه (شمس الدين، 2019).

ونرى أن الطريقة التي حصل بها الجاني على بيانات الضحية تُعدُّ من المؤشرات إلى القصد الجنائي، خصوصًا إذا تمت بطريقة غير مشروعة، مثل: اختراق هاتف الضحية.

وللتبسيط، يوضح جدول 1 أركان جرائم التزييف العميق، بالتطبيق على نص المادة 26 من القانون المصري رقم 175/ 2018 التي عاقبت من تعمد استعمال برنامج أو تقنية في معالجة معطيات شخصية للغير لربطها بمحتوى منافٍ للآداب العامة، أو لإظهارها بطريقة من شأنها المساس باعتباره وشرفه.

وإذا انتفى القصد الجنائي ترتبت مسئولية مدنية تقصيرية عن الإضرار بالغير، وللمتضرر الحق في رفع دعوى للتعويض (هيا، 2023).

ويتضح لنا، احتياج جريمة التزييف العميق إلى كل دليل يمكن الحصول عليه لإكمال أركان الجريمة، وقد فرضت البيئة الرقمية معايير فنية خاصة، وضوابط إجرائية معينة، وهو ما نتناوله في الفرع الثاني.

2. 2. 2. الأدلة الرقمية لإثبات جرائم التزييف العميق

2. 2. 2. 1. مفهوم الدليل الرقمي

الدليل الرقمي هو أي معلومات تُجمع أو تُحلل باستخدام برامج أو تقنيات متخصصة، ويشتق من أنظمة المعلومات، أو الشبكات، أو الأجهزة، أو الأدوات الرقمية (Arshad, et al., 2018).

وعرفه قانون مكافحة جرائم تقنية المعلومات المصري بأنه كل معلومة إلكترونية تتمتع بقيمة للإثبات، سواء مخزنة أو منقولة أو مستخرجة من أجهزة أو شبكات معلوماتية.

أما نظام الإثبات السعودي (1443هـ) فعرفه بأنه المُستخلص من بيانات مُنشئة أو مُصدرة أو مُستقبلة أو مُخزنة أو مُرسلة عبر الوسائل الإلكترونية. وتشمل السجلات والوثائق والتوقيعات والمراسلات، ووسائل الاتصال، والوسائط الإلكترونية، وأي شكل آخر من أشكال الأدلة الرقمية.

ويتضح لنا مرونة التشريع السعودي عند تعريف الدليل الرقمي، من خلال النص صراحةً على أي شكل من أشكال الأدلة الرقمية.

2. 2. 2. 2. الضوابط الإجرائية للدليل الرقمي في جرائم التزييف العميق

تُقيم صحة وجودة الأدلة الرقمية بدقة لتجنب نتائج غير عادلة، ويجب أن تكون سليمة وموثوقة، وأن تخضع للشروط الفنية (Arshad et al., 2018).

ففي مصر، حددت المادة (9) من اللائحة التنفيذية لقانون مكافحة جرائم تقنية المعلومات خمسة شروط إجرائية حتى يكون للدليل الرقمي القيمة الإثباتية للأدلة الجنائية المادية، منها أن يتصل مباشرة بالواقعة، وأن تُوثق مواصفاته وطرق التعامل معه في محضر إجراءات، ويتم فحصه وجمعه بواسطة مأموري الضبط القضائي، أو الخبراء والفنيين المعينين. ووضعت المادة الشروط الفنية الآتية:

- أن تُستخدم تقنيات للحصول على الدليل تمنع إتلافه أو تغيره، وأدوات موثوقة مثل: تقنية الحماية من التغيير (Write Block-er)، وتقنية توليد البصمة الرقمية (Digital Images Hash).
- أن يوثق نوع ومواصفات البرمجيات والأجهزة المستخدمة والكود الناتج عن التحقق الرقمي (Hash code) والخوارزمية المطبقة بمحاضر الضبط أو التقارير الفنية.

وفي المملكة، عدَّ المشرع الدليل الرقمي دليلًا أصليًّا وفقًا للمادة (55) من نظام الإثبات، وأخضعته لقواعد الإثبات بالكتابة. ونصت المادة (57) على حجية الأدلة الرقمية غير الرسمية إذا صدرت وفق نظام التعاملات الإلكترونية، أو نظام التجارة الإلكترونية، أو إذا استخلصت من وسيلة رقمية منصوص عليها صراحةً في عقد مبرم بين الأطراف، أو إذا كان مصدرًا رقميًّا شائعًا. ونصت المادة (59) على أنه بخلاف الحالات السابقة، يكون للدليل الرقمي قوة الإثبات المقررة للمحرر العادي، وفقًا لأحكامه الواردة في الباب الثالث.

ويتضح لنا، مرونة التشريعين في التعامل مع الدليل الرقمي؛ إذ أضاف السعودي أي شكل من الأدلة الرقمية ضمن التعريف، بينما تناول المصري باللائحة الأدوات على سبيل المثال لا الحصر، واشترط الموثوقية وضمان عدم الإتلاف أو التعديل. ويُضفي ذلك حجية قانونية للعلامة المائية الرقمية غير المرئية للإثبات.

كما تتجلى أهمية نشر الإرشادات القانونية لحفاظ الضحايا على الأدلة، وعدم إجراء فحوصات بمعرفتهم، فقد يؤدي سوء التعامل إلى إتلافها، وضعف حجيتها، وعدم صلاحيتها إجرائيًّا.

3. الإطار القانوني لمواجهة الجرائم الناشئة عن التزييف العميق

بعدما تناولنا المنظور القانوني للجرائم الناشئة عن التزييف العميق، ينبغي لنا البحث عن الإطار القانوني بمصر والمملكة لمواجهتها، وآليات تمكين جهات التحقيق من ملاحقة الجناة على المستويين الوطني والدولي.

3. 1. نظرة عامة على الحماية التشريعية للمصالح العامة والخاصة من تهديدات التزييف العميق

أدَّى تعدد أنماط الجرائم إلى ضرورة اتسام القواعد القانونية بالعموم لحماية المصالح العامة والخاصة من أي انتهاك يتم بأي وسيلة، بما فيها التزييف العميق. وتُعدُّ التشريعات في المملكة العربية السعودية وجمهورية مصر العربية ثرية بالنصوص الحامية لتلك المصالح. وفيما يأتي عرض لأهم ما له صلة بالتزييف العميق.

3. 1. 1. الأطر القانونية لمواجهة الجرائم الناشئة عن التزييف العميق بالمملكة العربية السعودية

جرَّمت المادة الثالثة من نظام مكافحة الجرائم المعلوماتية الدخول غير المصرح به إلى موقع أو نظام إلكتروني للتهديد أو الابتزاز، أو لتغير أو تدمير الموقع. وجرمت التشهير أو الإضرار بالآخرين عبر الوسائل التقنية المختلفة. وعاقبت المادة الرابعة من يستولي على مال منقول أو سند أو توقيع، بالاحتيال، أو اتخاذ اسم كاذب، أو انتحال صفة.

كما أعطى الحماية للمال المنقول والسندات والتوقيعات من الاحتيال، أو اتخاذ اسم كاذب أو انتحال صفة غير صحيحة، وهو ما يتوافق مع نص المادة الأولى من نظام مكافحة الاحتيال المالي وخيانة الأمانة (1442هـ) التي عاقبت كلَّ من يعتدي على مال مملوك للغير دون وجه حق، من خلال قيامه بفعل أو أكثر يتضمن أيًّا من طرق الاحتيال، مثل: الكذب، أو الخداع، أو الإيهام.

ووفر المشرع حماية للخصوصية والآداب العامة والحياة الخاصة بموجب المادة (6) من نظام مكافحة الجرائم المعلوماتية، التي عاقبت كلَّ من ينتج أو يعد أو يرسل أو يخزن أي محتوى أو موقع، أو مادة عبر الشبكة المعلوماتية، أو أجهزة الحاسب الآلي، إذا كان من شأنه المساس بالنظام العام، أو القيم الدينية أو الآداب العامة، أو حرمة الحياة الخاصة.

وإدراكًا من المشرع السعودي لأهمية تحقيق عنصر الردع من العقوبة، فقد أضاف للمادة سالفة الذكر تعديلًا ينص على جواز نشر ملخص الحكم الصادر بالعقوبة في صحيفة أو أكثر من الصحف المحلية، أو أي وسيلة أخرى مناسبة، حسب نوع الجريمة المرتكبة وجسامتها وتأثيرها.

3. 1. 2. الأطر القانونية لمواجهة الجرائم الناشئة عن التزييف العميق بجمهورية مصر العربية

تناول المشرع في الباب الثالث من القانون 175/ 2018 الجرائم والعقوبات، وجرَّمت المادة (13) و(14) الانتفاع غير المشروع بخدمات الاتصالات وتقنيات المعلومات، وعاقبت من يحصل دون وجه حق على خدمة منهما، بما فيها خدمات البث السمعي والمرئي، ومن يدخل عمدًا إلى موقع أو حساب أو نظام بطريقة غير مشروعة، أو دخل إليه دون قصد واستمر داخله.

وعاقبت المادة (23) من يستخدم الشبكة المعلوماتية، أو أي وسيلة تقنية للوصول غير المشروع إلى أرقام أو بيانات خاصة ببطاقات البنوك، أو أدوات الدفع الإلكتروني، وأغلظ المشرع العقوبة متى كان

والقصد استخدام تلك البيانات في الاستيلاء على أموال المجني عليه، أو للحصول على خدمات يتلقاها.

وتجدر الإشارة إلى المادة (32) من قانون العقوبات (1937) التي نصَّت على تطبيق العقوبة الأشد دون غيرها في حالة تعدد الجرائم التي ارتكبت لنفس الغرض، وكانت مترابطة. مثلًا، إذا استخدم الجاني التزييف العميق للوصول إلى بيانات بطاقات الدفع الإلكتروني للضحية، ثم استولى على أمواله، فهو بذلك قد ارتكب جريمتين تستوجبان تطبيق العقوبة الأشد بينهما، دون تعدد في العقوبة عن كل نتيجة.

ويكمل هذا الإطار نص المادة (336) من قانون العقوبات التي عاقبت كلَّ من يستولى على أموال منقولة، أو سندات أو ممتلكات مملوكة للغير من خلال طرق الاحتيال والخداع، أو باستخدام اسم مزيف أو صفة غير حقيقية. ونلاحظ أن هذا النص لم يقيد الاحتيال بطريقة محددة.

وشددت المادة (34) من قانون 175/ 2018 العقوبة إذا مس الفعل النظام أو الأمن القومي. ومن ثمَّ، فإن استخدام تقنيات التزييف العميق في ارتكاب الجرائم المعلوماتية يُعدُّ من صور هذا الإضرار، خاصة إذا استخدمت في بث محتوى مزيف لإثارة الفوضى أو هز الثقة في مؤسسات الدولة أو تأخير عملها، أو تهديد السلم والأمن في المجتمع، أو التحريض على الكراهية، أو التأثير على أحكام الدستور والقوانين.

وفي ختام المطلب، يتضح لنا اتساع نطاق التجريم عن الاستخدام الخبيث للتزييف العميق في النصوص القانونية بمصر والمملكة التي ضمنت الحماية للمصالح العامة والخاصة من الاعتداء المادي والرقمي، دون تحديد وسيلة أو طريقة أو نمط معين لارتكابها، وشددت العقوبة عند التأثير على الأمن الاقتصادي أو الاجتماعي. ويعكس ذلك مرونة التشريعات بالدولتين لحماية المصالح العامة والخاصة، سواء أكانت مادية أو رقمية، بما يواكب التحديات التي يفرضها التزييف العميق، ويضمن المساءلة القانونية عن الاستخدام الخبيث، ويحقق توازنًا بين حرية الاستخدام والحفاظ على الحقوق وأمن المجتمع.

3. 2. الضوابط القانونية لملاحقة مرتكبي جرائم التزييف العميق محليًّا ودوليًّا

تتطلب الطبيعة التقنية المعقَّدة للتزييف العميق تعاونًا مشتركًا بين سلطات إنفاذ القانون ومزودي الخدمات لملاحقة الجناة، كما تحتاج إلى تعاون تقني وتشريعي على المستويين الوطني والدولي. وهو ما نتناوله في هذا المطلب.

3. 2. 1. التزامات وواجبات المتحكم وصلاحيات جهات التحقيق بالمملكة العربية السعودية وجمهورية مصر العربية

3. 2. 1. التزامات وواجبات المتحكم وصلاحيات جهات التحقيق بالمملكة العربية السعودية

يشكل نظام حماية البيانات الشخصية إطارًا لحماية البيانات ومعالجتها ونقلها والإفصاح عنها، بما فيها من صور ثابتة وفيديوهات متحركة.

وقد منحت المادة (4) و(5) لصاحب البيانات الحق في العلم، وإحاطته بالمسوغ النظامي لجمع بياناته الشخصية والغرض منها. وعدم جواز معالجتها أو تغيير الغرض من معالجتها إلا بعد موافقته.

وعرف النظام جهة التحكم بأنها الجهة العامة أو الخاصة، التي تتولى تحديد الغرض من المعالجة، سواء باشرتها بنفسها، أو من خلال جهة أخرى. ونصت المادة (10) على عدم جواز قيام الجهة بجمع البيانات الشخصية إلا من صاحبها مباشرة، ولا يجوز لها عكس ذلك إلا بموافقته، أو لو كانت متاحة للعموم، أو جرى جمعها من مصدر متاح للعموم.

ويظهر ذلك أهمية الدور الواقع على الجهات العامة والخاصة في نشر الوعي والدراية، وتقديم الإرشادات والنصائح التي تؤكد أن حماية البيانات الشخصية تبدأ من الإجراءات التي يتخذها الشخص نفسه، وأن إتاحته لبياناته الشخصية على مصادر متاحة للعموم هي موافقة ضمنية منه على استخدامها.

ووضع النظام أحكامًا وضوابط تنظم المعالجة، وتضمن بشكل كافٍ الخصوصية وعدم الإضرار بصاحبها بأي شكل.

وقدمت سدايا (2024) دليلًا ارشاديًّا لحالات إفصاح المتحكم عن البيانات الشخصية في ضوء أحكام النظام ولائحته التنفيذية، وأكدت إلزامه بالإفصاح إذا طلبت جهة عامة ذلك لأغراض أمنية أو للمصلحة العامة أو لاستيفاء متطلبات قضائية، بما في ذلك الكشف عن عمليات الاحتيال وحماية أمن الشبكة والمعلومات.

ويؤكد ذلك امتلاك جهات التحقيق والسلطات القضائية الحق في الحصول على بيانات المشتبه بهم، والتزام المتحكم بالحد الأدنى من الإفصاح، وتوفير الضمانات الكافية للحفاظ على الخصوصية.

ونصت الفقرة 1 من المادة (36) على عقوبة من يخالف أحكام النظام بالإنذار أو الغرامة، دون الإخلال بأي عقوبة أشد مقررة في نظام آخر، وأجازت مضاعفة الغرامة إذا تكررت المخالفة.

3. 2. 1. 2. التزامات وواجبات المتحكم وصلاحيات جهات التحقيق بجمهورية مصر العربية

نصت المادة (26) من قانون حماية البيانات الشخصية على ضرورة موافقة صاحب البيانات على المعالجة. وألزمت المادة (2) من قانون

مكافحة جرائم تقنية المعلومات مقدمي الخدمة بتوفير ما يلزم عند طلب الجهات المختصة بالأمن القومي تمكينهم من أداء مهامهم، في إطار احترام حرمة الحياة الخاصة التي يكفلها الدستور. وعاقبت المادة (33) من يخل بما ورد في تلك الفقرة.

ويعكس ذلك إدراك المشرع المصري لخطورة امتناع مقدم الخدمة عن التعاون مع جهات الأمن القومي في التحقيقات المتعلقة بالجرائم.

ومنحت المادة (6) جهة التحقيق صلاحية تفويض مأموري الضبط القضائي بضبط أو سحب أو جمع، أو التحفظ على البيانات والمعلومات أو تتبعها، أيًّا كانت وسيلة تخزينها، وأتاحت لها حق الدخول والتفتيش والاطلاع على الأنظمة وقواعد البيانات والبرامج. وألزمت مقدم الخدمة بتسليم أي بيانات تخص التقنيات التابعة له، وعاقبته المادة (32) إذا امتنع عن التعاون مع جهة التحقيق المختصة.

وعلى الرغم من ذلك، فلا يخضع المزود أو المتحكم خارج النطاق الجغرافي لمصر أو المملكة لتلك الالتزامات؛ مما يتطلب تعاونًا دوليًّا مشتركًا نتناوله في الفرع الثاني.

3. 2. 2. التعاون الدولي في مجال مكافحة جرائم التزييف العميق

يتجلَّى لنا مما سبق، أهمية التعاون الدولي بين الأطراف المعنية لتنظيم عملية اكتشاف المحتوى المزيف.

وقد دعا (Fabuyi, et al., 2024) إلى ضرورة التعاون بين صانعي السياسات وشركات التكنولوجيا والمجتمع المدني في صياغة وتنفيذ إستراتيجيات فعَّالة للتخفيف من الآثار الضارة للمحتوى المزيف. وأن يتضمن هذا التعاون تعزيز التدابير القانونية والتنظيمية، ويحفز الابتكارات القادرة على كشف المحتوى المزيف.

وتحاول الدول وضع الضوابط العامة للشركات لإضفاء معايير الشفافية إلى المحتوى المزيف، كما سبق الإشارة. وفي سبيل ذلك، تسعى الشركات الرائدة إلى التعاون لتطوير حلول تكنولوجية مبتكرة لتعزيز مستويات الأمان وضمان الامتثال. وأطلقت مؤسسة التطوير المشترك The Joint Development Foundation (2025) تحالفًا يسمى «تحالف منشأ المحتوى وأصالته (C2PA,2025)، الذي يجمع عدة شركات لوضع المواصفات الفنية الموحدة اللازمة لتحديد مصدر المحتوى وأصالته. ويعمل هذا التحالف باستمرار على تحديث هذه المواصفات استجابةً للتطورات السريعة في مجال الذكاء الاصطناعي. ويتعاون ذلك التحالف مع مبادرة أصالة المحتوى Content Authenticity Initiative (CAI, 2025)، التي أعلنت التزامها بالشفافية وتتبع مصدر المحتوى وصحته. وتحاول توفير أدوات لدعم هذه الأهداف للجمهور.

وفي مصر، نصَّت المادة (4) من القانون 2018/175 على أن تُيسر الجهات المصرية المختصة التعاون مع نظيراتها في الدول الأجنبية بموجب اتفاقيات دولية أو إقليمية أو ثنائية مُصدّق عليها، أو بناءً على مبدأ المعاملة بالمثل. ويشمل هذا التعاون تبادل المعلومات لمنع ارتكاب الجرائم التقنية، والمساعدة في التحقيقات، وتعقب مرتكبيها (مرعي، 2022).

وأبرمت المملكة العربية السعودية اتفاقيات ثنائية ودولية لمكافحة الجرائم الإلكترونية، منها وثيقة الرياض للنظام الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون لدول الخليج العربية (2013). التي حددت إطارًا للتعاون في هذا المجال داخل دول مجلس التعاون.

ولا شك في أن الخصائص التي تتمتع بها العلامة المائية الرقمية غير المرئية تُعزز من موثوقيتها، إلا أنها تحتاج إلى مزيد من التعاون بين الشركات التقنية الرائدة لتوفير أداة موحدة لكشف المحتوى المولد عبر أي مزود، وتوفير أداة مغلقة المصدر لتمكين جهات التحقيق من تتبع الجناة.

4. النتائج

- يتسع نطاق التجريم في تشريعات مصر والمملكة ليحمي المصالح العامة والخاصة، المادية والرقمية، ويحمي إطارهما القانوني البيانات الشخصية التي تُستخدم في التزييف العميق، لكن سلوك ومشاعر البشر لم يتمتعا بالحماية صراحةً.
- لم تتناول التشريعات المصرية والسعودية تعريفًا صريحًا لتقنية التزييف العميق، إلا أنهما وضعا تعريفات تتيح للمحكمة مرونة لتكييفها وفقًا لملابسات القضية المطروحة. وسدت الهيئة السعودية للبيانات والذكاء الاصطناعي تلك الفجوة بتقديم كتيبات إرشادية، منها مبادئ التزييف العميق.
- بدأ الاتحاد الأوروبي تجاه تنظيم الذكاء الاصطناعي، وصنف أنظمة التزييف العميق ضمن المخاطر المحدودة، التي تحتاج إلى إلزام الأطراف الفاعلة باتخاذ تدابير تعزز من الشفافية والمصداقية، منها تضمين العلامة المائية الرقمية.
- تستخدم جهات التحقيق الأدوات مفتوحة المصدر بخلاف مغلقة المصدر، وتخضع إلى ضوابط إجرائية مُحددة، يؤدي الإخلال بها إلى بُطلانها، أهمها موثوقيتها.
- للعلامة المائية الرقمية موثوقية في كشف المحتوى المُزيف المرئي والصوتي، وحجية في الإثبات الجنائي بالتشريع المصري والسعودي.

- قد يُضعف عبث الضحايا بالأدلة الرقمية أو فحصها بمعرفتهم من صحتها كدليل رقمي موضوعيًّا وإجرائيًّا.
- أتاح المشرع المصري والسعودي صلاحيات كافية لجهات التحقيق لملاحقة الجناة داخل النطاق الجغرافي، وسنا نصوصًا للتعاون مع الجهات الأجنبية.
- وضع المشرع المصري والسعودي ضوابط وأحكامًا تلزم المتحكم في البيانات ومقدم الخدمة بالإفصاح عند طلب جهات التحقيق، دون الإخلال بخصوصية المستخدمين.
- الجريمة الناشئة عن التزييف العميق من الجرائم العابرة للحدود، ومن الضروري وضع ضوابط عالمية ومعايير تقنية موحدة، ودعم جهات التحقيق بآليات موثوقة.

وقد ضمن الإطار القانوني المصري والسعودي حماية المصالح من الاعتداء عليها عبر التزييف العميق، ووفرا أحكامًا تلزم المتحكم بالإفصاح للقضاء وجهات التحقيق، ومنحا جهات التحقيق صلاحيات لتمكينهم من التفتيش والضبط، وأتاح المشرع بالدولتين مساحة كافية لتكيف المحكمة السلوك المُرتكب، وحددا ضوابط صريحة للتعامل مع الأدلة الرقمية، إلا أن الأمر ما زال يحتاج إلى مزيد من التعاون على المستوى الدولي، بجانب نشر الوعي القانوني بمخاطر التزييف العميق وأمن البيانات وسلامتها وكيفية التعامل مع الأدلة الرقمية.

5. التوصيات

توصي الدراسة المشرع المصري والسعودي بما يأتي:

- ضم سلوك ومشاعر الشخص الطبيعي بشكل صريح ضمن نطاق تعريف البيانات الشخصية الحساسة، التي يستدل من خلالها على هويته.
- دفع مزودي الخدمة نحو تضمين العلامة المائية الرقمية غير المرئية في المحتوى المزيف، مع وضع معايير تقنية تعزِّز من فاعليتها، وتمكن جهات التحقيق من ملاحقة الجناة.
- تحفيزهم للالتزام بالمسئولية المجتمعية في نشر الوعي لدى الجمهور، وبمعايير الأمن والسلامة، والاستخدام المسئول للتقنية.
- تحديد تعريفات قانونية مُحددة للأطراف الفاعلة في سلسلة قيمة الذكاء الاصطناعي، فعلى الرغم من تحمل المستخدم النهائي المسئولية عن الاستخدام، فإن وجود تعريفات لكل الأطراف يُمكن من تحميلها مسئوليات تُعزز من الشفافية وتزيد من تمكين جهات التحقيق قانونًا.
- زيادة البرامج التوعوية لدى المجتمع المصري والسعودي، للتأكيد على أن حماية البيانات الشخصية تبدأ من الإجراءات التي يتخذها الشخص نفسه، وأن إتاحتها على مصادر عامة هي موافقة ضمنية منه على استخدامها.
- توصي الدراسة المجلس الوطني المصري للذكاء الاصطناعي بإصدار كتيب إرشادي عن الاستخدام المسئول لأدوات التزييف العميق، وتوضيح مسئوليات الأطراف الفاعلة، على غرار ما تقدمه سدايا من كتيبات إرشادية

الإفصاح عن تضارب المصالح

يقر المؤلف أنه ليس لديه أي تضارب في المصالح لهذا البحث.

الإفصاح عن تمويل البحث

يقر المؤلف بأن هذا البحث لم يتلقَّ أي منحة ماليَّة، من أي جهة تمويل في القطاعات الحكوميَّة، أو التجاريَّة، أو المؤسسات غير الربحية.

المراجع

المراجع العربية

حسني، محمود نجيب. (1983). علاقة السببية في قانون العقوبات. القاهرة: دار النهضة العربية.

زكير، أحمد عبد الموجود أبوبكر. (2022). جريمة التزييف الإباحي العميق دراسة. مقارنة. المجلة القانونية، كلية الحقوق، جامعة القاهرة، 2227.

سدايا. (2022). مبادئ التزييف العميق. الرياض: الهيئة السعودية للبيانات والذكاء الاصطناعي سدايا.

سدايا. (2024). الدليل الاسترشادي لحالات الإفصاح عن البيانات الشخصية، الرياض، المملكة العربية السعودية، الهيئة السعودية للبيانات والذكاء الاصطناعي، سدايا.

شمس الدين، أشرف توفيق. (2019). شرح قانون العقوبات، القسم العام، النظرية العامة للجريمة. القاهرة: دار النهضة العربية.

العجيل، منصور عبد السلام عبد الحميد حسان. (2021). الضوابط القانونية للإثبات الجنائي بالأدلة الرقمية: دراسة مقارنة، المجلة القانونية، جامعة القاهرة، 3341 - 3414.

أبو العلا، أشرف سيد، (2024). المواجهة الجنائية لتقنية الديب فيك. مجلة العلوم القانونية والاقتصادية، 477 - 511.

فؤاد، درويش، حسنين. (2025). المنظور القانوني والأخلاقي لحوكمة الذكاء الاصطناعي وإدارة مخاطره. القاهرة: دار مصر للنشر والتوزيع.

قانون الإجراءات الجنائية رقم 150 لسنة 1950، مصر.

قانون العقوبات رقم 58 لسنة 1937، مصر.

قانون رقم 151 لسنة 2020 بشأن حماية البيانات الشخصية، مصر.

قانون رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، مصر.

القهوجي، علي عبد القادر (2003). الحماية الجنائية للكيان المعنوي للحاسب الآلي من خلال حق المؤلف، المؤتمر العلمي الأول حول الجوانب القانونية والأمنية للعمليات الإلكترونية، دبي.

اللائحة التنفيذية لقانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، الجريدة الرسمية، العدد 35 تابع (ج)، 27 أغسطس، 2020. مصر.

مجلس التعاون لدول الخليج العربية. (2013). وثيقة الرياض للنظام الموحد لمكافحة جرائم تقنية المعلومات لدول مجلس التعاون لدول الخليج العربية.

مرعي، أحمد لطفي السيد، الأدلة الرقمية المتحصلة من التفتيش الجنائي الإلكتروني (دراسة مقارنة)، مجلة الدراسات القانونية والاقتصادية، مجلد 8، ع 1، 2022، ص. 290 - 368.

مركز حقوق الإنسان. (2024). بروتوكول بيركلي بشأن التحقيقات الرقمية مفتوحة المصدر (مكتب المفوض السامي لحقوق الإنسان بالأمم المتحدة؛ مركز حقوق الإنسان، كلية الحقوق بجامعة كاليفورنيا - بيركلي). الأمم المتحدة.

النجار، سحر فؤاد مجيد. (2024). المواجهة الجنائية للجرائم الناشئة عن استخدام تقنية التزييف العميق. Journal of Legal Sciences, 39)، 633 - 575.

نظام الإثبات السعودي الصادر بالمرسوم الملكي رقم (م/43) وتاريخ 1443/5/26هـ.

نظام حماية البيانات الشخصية السعودي، الصادر بالمرسوم الملكي رقم (م/19) بتاريخ 1443/2/9هـ، والمعدل بالمرسوم الملكي رقم (م/148) بتاريخ 1444/9/5هـ.

نظام مكافحة الاحتيال المالي وخيانة الأمانة الصادر بمرسوم ملكي رقم (م/79) وتاريخ 1442/9/10هـ بتاريخ 2021/4/22م.

نظام مكافحة جرائم المعلوماتية السعودي الصادر بالمرسوم الملكي رقم م/17 بتاريخ 1428/3/8 هـ الموافق 2007/3/27م.

هيا محمد شاهين طوق البوعينين. (2023). الجهل بالقانون وأثره على المسؤولية الجنائية والمدنية، مجلة بحوث الشرق الأوسط 11(88) 3-4 .

المراجع الأجنبية

Agarwal, S., Farid, H., Gu, Y., He, M., Nagano, K., & Li, H. (2019, June). Protecting world leaders against deep fakes. In CVPR workshops (Vol. 1, No. 38).

Ahmed, A. M., Abdelrazek, M., Aryal, S., & Nguyen, T. T. (2023). An overview of Eulerian video motion magnification methods. Computers & Graphics, 145 - 163.

Altuncu, E., Franqueira, V. N., & Li, S. (2022). Deepfake: definitions, performance metrics and standards, datasetes and a meta-review. Frontiers in Big Data, Sec. Cybersecurity and Privacy 7, 1 - 23.

Arshad, H., Jantan, A. B., & Abiodun, O. I. (2018). Digital Forensics: Review of Issues in Scientific Validation of Digital Evidence. Journal of Information Processing Systems, pp. 346 - 376.

Berkely Protocol. (2024). Berkeley Protocol on Digital Open Source Investigations. Berkely Protocol. UNHRC & UC Berkely School of Law.

C2PA. (2025). Coalition for Content Provenance and Authenticity C2PA.

CAI. (2025). Content Authenticity Initiative.

California Legilative Information (2023-2024) SB-942 California AI Transparency Act.

California State. (April, 2024). legistration, Amendement to california assembly bill 3211. https://legiscan.com/CA/text/ AB3211/id/2984195. California State Legislature.

Cambridge Dictionary.

Casey, E., & Others. (2010). Handbook of digital forensics and investigation. California: Elsevier Inc.

Christodorescu, M., Mihai, Craven, R., Feizi, S., Gong, N., Hoffmann, M., . . . Jiang, Z. (2024, 5 21). Securing the future of genAI: Policy and technology. Retrieved from https://arxiv.org/abs/2407.12999

Citron, D. K., & Chesney, R. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review, 1762.

tions: Emerging threats and potential mitigations. Georgetown University's Center for Security and Emerging Technology OpenAI and Stanford Internet Observatory.

Janiesch C, Zschech P, Heinrich K (2021) Machine learning and deep learning. Electron Mark 31(3):685–695

McGEE, S. (2022). Evidence-Based Physical Diagnosis. Philadephia: Elsevier.

Riley, J. (2017). Undrstanding Metadata. Washington DC, United States.: National Information Standards Organization.

Sensity. (2024). The state of deepfakes.

Stanford University (2023). AI Index Report.

The Joint Development Foundation.(2025).

Wadhera, S., Kamra, D., Rajpal, A., Jain, A., & Jain, V. (2022, July 7). A Comprehensive Review on Digital Image Watermarking.

Wu, X., Liao, X., Ou, B., Liu, Y., & Qin, Z. (2024). Are watermarks bugs for deepfake detectors? rethinking proactive forensics. Proceedings of the Thirty-Third International Joint Conference on Artificial Intelligence (IJCAI-24) (pp. 6089 - 6097). Jeju: Proceedings of the Thirty-Third International Joint Conference on Artificial Intelligence (IJCAI-24).

European Parliament, AI Investment: EU and Global Indicators; Statista, 2023, Standord AI Index Report (2024).

Fabuyi, J., Olaniyi, O. O., Olateju, O., Aideyan, N. T., Selsi-Aina, O., & Olaniyi, F G. (2024). Deepfake Regulations and Their Impact on Content Creation in the Entertainment Industry. Archives of Current Research International 24, pp. 10-0734.

Fernandez, P. L. (2024). What Lies Ahead for Generative AI Watermarking. Tech. Rep., 1

Fernandez, P., Couairon , G., Jégou, H., Douze, M., & Furon, T. (2023). The Stable Signature: Rooting Watermarks in Latent Diffusion Models. Fernandez, P., Couairon, G., Jégou, H., Douze, M., & Furon, T. (2023). The stable signature: Rooting watermarks in latent diffusion models. In Proceedings of the IEEE/CVF International Conference on Computer Vision (pp. 22466-22477). Paris: International Conference on Computer Vision.

Giovanni Spitale, Andorno, N. B., & Germani, F (2023). Ai model gpt-3 (dis) informs us better than humans. Science Advances 9, 1 - 29.

Goldstein, J. A., Sastry, G., Musser, M., DiResta, R., Gentzel, M., & Sedova, K. (2023). Generative language models and automated influence opera-