Criminal Response to Crimes Stemming from the Use of Deepfake Technology

Sahar Fouad Majeed Al- Najar
University of Baghdad - College of Law

mrs.sahar@colaw.uobaghdad.edu.iq

Received Date: 10/11/2024. Accepted Date: 2/12/2024. Publication Date: 25/12/2024.

Abstract

Cybercrime is rapidly evolving as technology advances and reaches new dimensions in a way that blurs the lines between what is real and what is simulated. Deepfake technology has become part of cybercrime. Deepfake technology has similar features to CGI technology (Computer Generated Image) in the film industry, making it possible to create videos - images and audio using artificial intelligence arms in a way that is so realistic and difficult for humans to recognize it as fake. This poses serious risks, with potential consequences ranging from unfair electoral practices to the use of forged evidence in court. This technology first emerged in 2017 on a social media platform called *Reddit*. Although this technology has many legitimate uses, its illegitimate uses are more prominent, resulting in the infringement of legally protected interests. Therefore, the emergence of this technology calls for serious thinking about the serious violations of legally protected interests. Therefore, the criminal legislature must re-adapt the legal rules with a realistic-

material meaning, in order to deal with an intangible virtual reality and attempt to criminalize the behaviors resulting from this technology. In addition, the legislature must pay attention to the policies of prevention and protection from crimes arising from deepfake.

Keywords: Deepfake, Publicity, Revenge Porn, Legal Confrontation.

المواجهة الجنائية للجرائم الناشئة عن إستخدام تقنية التزييف العميق

سحر فؤاد مجيد النجار*
جامعة بغداد – كلية القانون
mrs.sahar@colaw.uobaghdad.edu.iq

تاريخ الاستلام: 2024/11/10. تاريخ القبول: 2024/12/2. تاريخ النشر: 2024/12/25.

المستخلص

تتطور الجرائم الإلكترونية بسرعة مع تقدم التكنولوجيا وبلوغها أبعادًا جديدة بطريقة تطمس الخطوط الفاصلة بين ما هو حقيقي وما هو مُحاكى. أصبحت تقنية التزييف العميق Deepfake جزءًا من الجرائم الإلكترونية. تتميز تقنية التزييف العميق Deepfake بأن لها ميزات مماثلة لتقنية CGI (Computer Generated Images)في نطاق صناعة السينما، مما يجعل من الممكن إنشاء مقاطع فيديو أو صور باستخدام أذرع الذكاء الإصطناعي وبطريقة واقعية للغاية يصعب على البشر التعرف عليها على أنها مزيفة. وهذا يفرض مخاطر جسيمة، مع عواقب محتملة تتراوح من ممارسات إنتخابية غير عادلة إلى إستخدام أدلة مزورة في المحكمة. لقد ظهرت هذه التقنية لأول مرة في عام 2017 في منصة التواصل الإجتماعي التي تسمى *Reddit*. وعلى الرغم من أن هذه التقنية لها العديد من الإستخدامات المشروعة، إلا أن إستخدامتها غير المشروعة أكثر بروزًا، مما نتج عنها المساس بالمصالح المحمية قانونًا. لذا يؤدي ظهور هذه التقنية التفكّير بشكلً جديً حول الإنتهاكات الخطيرة للمصالح المحمية قانونًا. لذا يتحتم على المُشرع الجزائي إعادة تكييف القواعد القانونية ذات المدلول الواقعي – المادي، من أجل التعامل مع واقع إفتراضي غير ملموس ومحاولته تجريم السلوكيات الناجمة عن هذه التقنية. فضلًا عن الإهتمام بسياستي المنع والوقاية من الجرائم التي تنشأ عن التزييف العميق.

الكلمات المفتاحية: التزييف العميق- العلانية – الانتقام الاباحي – المواجهة القانونية.

---

*مدرس

المقدمة
Introduction

لقد بات لزامًا على القانون الجنائي أن يُواكب ما يُستجد من سلوكيات تُعد خطرًا على المصالح الجديرة بالحماية في الوقت الحاضر في ظلّ التسارع التكنولوجي وماينتج عنه من تقنيات حديثة التي قد يستغلها المجرمون في جرائمهم على الرغم من أهمية هذه التقنيات للجنس البشري. تُمثل تقنية التزييف العميق Deepfake أحدى التقنيات الحديثة الأكثر تطورًا في المجال التكنولوجي التي تستخدم الذكاء الإصطناعي وما له من خطورة في عالم التلاعب بالوسائط المتعددة، فتعتمد على تقنيات صناعة المقاطع الصوتية أو الفيديويه للشخصيات العامة أو غيرها، وذلك بالاعتماد على التعلم الآلي والعميق الذي يُمثل أحدى ميزات الذكاء الإصطناعي. ونتيجة للتطور الذي يتمتع به الذكاء الإصطناعي وقدرته على محاكاة العنصر البشري أدى إلى استخدامه بصورة غير سليمة فنجم عنه عمليات التزييف العميق ومايترتب عنها قلة أوإنعدام ثقة الجمهور بالمحتويات المسموعة أو المرئية وماينجم عنها من جرائم كالتشهير والإساءة للغير وإنتهاك الحق في الخصوصية والتضليل والمحتوى الزائف وغيرها.

أهمية البحث:Research Objective يعّد موضوع ،" **المواجهة الجنائية للجرائم الناشئة عن استخدام تقنية التزييف العميق**" من المواضيع الحديثة ومن الظواهر الإجرامية المستحدثة في مجال العلم الجنائي، ومثار نقاش فقهي وقانوني، ذلك لأن التطور المخيف في تكنولوجيا الإتصالات والذكاء الإصطناعي قد أحدث ثورة في مختلف الأصعدة، وكان له تداعيات إقتصادية – إجتماعية – جيوسياسية، وأنتقل الذكاء الإصطناعي من المفهوم الضيق ذو البعد الواحد (القدرة على القيام بمهام فردية كالتعرف على الوجه والترجمة مثلًا) إلى المفهوم العام متعدد المهام (القيام بمهام معقدة بطريقة تحاكي الأدمغة البشرية)، كما أن تطبيقات وتقنيات الذكاء الإصطناعي ومنها التزييف العميق ستكون مُستقبلًا رافدًا لإرتكاب مختلف الجرائم، كما ستكون سلاحًا خطيرًا وقليل الكلفة في الحروب الحديثة " الحروب السيبرانية".

مشكلة البحث :Research Problem تتجسد أشكالية البحث في مدى كفاية النصوص القانونية للدول بصورتيها التقليدية والمستجدة في مواجهة الجرائم الناجمة عن التزييف العميق للحد من هذه الجرائم التي تستخدام الذكاء الإصطناعي والتي تسبب اضرارًا جسيمة بالدولة – المؤسسات- الافراد، فضلًا عن بيان مفهوم التزييف العميق ومخاطره على المصالح المحمية قانونًا.

الهدف من الدراسة: **aim of the study** الإسهام في إثراء البحث العلمي القانوني بدراسة حديثة تبين مقدارالخطورة التي يشكلها التزييف العميق الذي يستخدام الذكاء

الإصطناعي من أجل نشر معلومات مضللة عن الغير او أنه أداة متكررة لإرتكاب عمليات الإحتيال المالية وخداع الأفراد والشركات للحصول على أموال وغيرها من الأهداف. أن هذا الموضوع لم يحضَ بإهتمام الباحثين في مجال القانون الجنائي، وقلة الدراسات التي تناولت الموضوع، فضلا عن بيان موقف الدول الغربية التي تعد متقدمة تشريعيًا عن الدول العربية في مواجهة الجرائم التي تستخدم هذه التقنية.

منهجية البحث: Research Methods سيتبنى هذا البحث المنهج التحليلي والإستقرائي للنصوص القانونية ذات الصلة بالموضوع، والمنهج الوصفي الذي يعتمد على جمع المعلومات والحقائق من مختلف المصادر التي تتعلق بتقنية التزييف العميق وسيكون نطاق البحث محصورًا في تشريعات الدول الغربية فقط.

ولغرض احتواء أشكالية البحث المطروحة، أرتأينا تقسيمه على مبحثين وعلى النحو الآتي:

المبحث الاول: ماهيّة تقنية التزييف العميق والمبحث الثاني: مدى كفاية الأُطر القانونية والتقنية في مواجهة جرائم تقنية التزييف العميق.

المبحث الاول: ماهيّة تقنية التزييف العميق.

The First Topic: What is Deepfake Technology

لقد ساهم الذكاء الإصطناعي في التفكير بشكل جديّ بكثير من المسائل التي لم يشهدْها العصر، منها، ربوتوتات الدردشة- المحادثات الشخصية المؤتمته، فضلًا عن تزييف مقاطع الفيديو والصور بطريقة يصعب التمييز بين الحقيقة والمحاكاة وغيرها، وتثير هذه التقنية ضررًا بالمصالح المعتبرة قانونًا في ظلّ وجود القصور التشريعي. ولبيان ماهية التزييف العميق، قسمنا المبحث على أربعة مطالب وعلى النحو الآتي:- المطلب الاول : مفهوم تقنية التزييف العميق، المطلب الثاني: الاثر السلبي لتقنية التزييف العميق في المجتمع، المطلب الثالث: سمات الجرائم المرتكبة بتقنية التزييف العميق، المطلب الرابع: التزييف العميق تهديد إجرامي.

المطلب الاول : مفهوم تقنية التزييف العميق.

The First Requirement: The Concept of Deepfake Technology.

يعد التزييف العميق أحد نتاجات تطبيقات تقنيات الذكاء الإصطناعي والذي يُدعى " Deep Learning Model" ، وأن هذا المصطلح الذي أنبثق للوجود في عام 2017 [1]، مزيج من كلمتي "التعلم العميق Deep Learning" و"المزيف Fake " ويُعرّف على أنه، شكل من أشكال المحتوى السمعي البصري الذي تم إنشاؤه أو التلاعب به

باستخدام الذكاء الإصطناعي (AI) الذي يصور شخصًا أو شيئًا بشكل خاطئ". غالبًا ما تظهر التزييفات العميقة أفرادًا في قطاعات الترفيه أو الموضة أو الرياضة بمحتويات مزيفة، وأن هناك قلقًا متزايدًا بشأن إنتشارها والتأثير الذي قد تحدثه في العملية الديمقراطية[2]. كما تُعرف على انها،" عملية تصنيع أو أختلاق الصور أو الفيديوات باستخدام انظمة الذكاء الإصطناعي، وغالبًا ما تكون باستخدام وجه أو صوت شخص ما بقصد عمل فيديو أو تسجيل صوتي يكون مشابه للفرد الذي يتم عمل التزييف العميق له سواء كان فيديو أو تسجيل صوتي." [3] ، كما يعني أنه ،"الإستخدام غير الشرعي لتقنية التعليم العميق" [4]، يرى جانبٌ من الفقه الفرنسي أن التزييف العميق ، يعني أستخدام برامج الذكاء الإصطناعي Artificial Intelligence (AI) لتزييف محتوى الصوت والفيديو إذ تتيح هذه التقنية إنشاء مقاطع فيديو مزيفة أو ‘‘التبديل الذكي للوجوه’’، والمعروفة بمقاطع الفيديو شديدة التزييف – عن طريق التلاعب بالصور والأصوات بإستخدام تقنية ‘‘التعلم العميق’’ويكون القصد من مقاطع الفيديو هذه، هو أن تكون قادرًا على جعل أي شخص يفعل أو يقول أي شيء. وإستنادًا لمفهوم البرلمان الآوروبي للتزييف العميق يرى أن له مدلولًا أوسع من الوسائط الإصطناعية والتي تقف عند حد تنميط البيانات الأصلية أو تعديلها، فوفقًا لمفهومهم فأن التزييف العميق يستهدف تقليد الصورة أو الفيديو أو انتاجها بواسطة أنظمة الذكاء الإصطناعي والذي لايمت للواقع بأي صلة عن طريق إستنساخ الصوت أو تحريف الصور أو تركيب النصوص[5]. إلى الأن، لايوجد تعريف واضح للتزييف العميق والذي يميز بين التزيف المشروع عن التزيف غير المشروع. وآخرون عرفوه، " أنه الفيديو الذي يتم إنتاجه بواسطة خورزميات التعلم العميق بواسطة برامج متاحة يُسهل الوصول إليها والتي تتمتع بقدرتها على إنتاج وتقديم محتوى مزييف يخالف الحقيقية عن طريق وضع وجه شخص"الضحية" على جسد شخص آخر بدون تمييز على حدوث ذلك،"[6] . أن اغلب التعريفات الواردة أعلاه تُركز على الخصائص التقنية الفنية لهذه التقنية، لذا فالحاجة تدعو لتنظيمها قانونيًا. ويرى الباحث، أن التزييف العميق أحد تطبيقات الذكاء الإصطناعي والتي لها القدرة على إنشاء محتويات رقمية (مرئية – صوتية) أو كليهما لشخص ما، بصورة تُحاكي الواقع وتُخالف الحقيقية في نفس الوقت، بقصد الإضرار به وتعريض المصالح المحمية قانونًا لضرر أو خطر.

ان التكنولوجيا التي تقف خلف إنشاء مقاطع التزييف العميق Deepfake [7] تتمثل بـــ **تقنية التعلم العميق (Deep Learning Technology)** للمحتوى السمعي والسمعي البصري. وعند استخدامها بشكل صحيح، يُمكن لهذه النماذج إنتاج محتوى يُظهر بشكل مقنع أشخاصًا يقولون أو يفعلون أشياء لم يفعلوها أبدًا، أو يضعون

أشخاصًا لم يكونوا موجودين في المقام الأول [8]، لذا نكون أمام مُحتوى منتج مزييف طبق الأصل ومُخالف للحقيقية تمامًا. **والتقنية الأُخرى، (GAN Network Generative Adversarial)**المستخدمة في الذكاء الإصطناعي المكتشفة من قبل *Ian Goodfellow* الباحث في شركة Google في عام 2014. يتم تشكيل GAN بإستخدام شبكتين مختلفتين معًا تتعلمان من بعضهما البعض من خلال التنافس بينهما. **الشبكة الأولى:** هي (Generator Network) شبكة المولد. يُمكن لشبكة المولد إنشاء صور وأصوات وبيانات واقعية من الضوضاء أو المتجهات، فتنتج بيانات أكثر اقناعًا للواقع. **والشبكة الثانية** هي (Discriminator Network) شبكة التمييز. تحاول هذه الشبكة التمييز بين البيانات الحقيقية والبيانات المُزيفة التي يُنتجها المُولد للمحتوى. وبالتالي، يزداد مُعدل التنبؤ الصحيح لشبكة التمييز، ويتم إنتاج صور أكثر واقعية وتستمر هذه العملية التنافسية بين هاتين الشبكتين حتى يتم خلق محتوى من قبل شبكة المولد يصُعب تميزه عن الحقيقية من قبل شبكة المميز[9]. بعبارة أخرى، تُستخدم شبكات GAN في إنتاج ملفات الوسائط مثل الصور والصوت والفيديو وقد يبدو هذا معقدًا للأشخاص الذين ليسوا على دراية كبيرة بالتكنولوجيا. ولكن اليوم، مع وجود عدد قليل من التطبيقات (FaceApp وReFaceApp وFaceMagic وما إلى ذلك) التي يُمكن تنزيلها على الهواتف الذكية، يُمكن إنشاء مقاطع فيديو Deepfake ببضع نقرات[10].

المطلب الثاني: الاثر السلبي لتقنية التزييف العميق في المجتمع.
The Second Requirement: The Negative Impact of Deepfake Technology on Society.

على المستويين الفردي والتنظيمي، تُتيح مقاطع الفيديو المزيفة أنشطة غير مشروعة مثل الأستغلال المالي عن طريق إساءة استخدام هوية شخص آخر، وإنتاج مواد إباحية بدون موافقة، والتي تؤدي إلى ضرر شديد بالسمعة ، والاحتيال بتسويق المنتجات للأفراد، وتشويه سمعة أعمال المنافسين، حيث وجدت دراسة في عام 2019 أن مقاطع الفيديو الإباحية الانتقامية تمثل 96% من جميع مقاطع الفيديو المزيفة [11]. فعلى سبيل المثال، إن الانتشار السريع لمقاطع الفيديو الإباحية المزيفة للممثلة الأمريكية تايلور سويفت إلى ملايين المشاهدات على منصة X خلال فترة قصيرة في يناير 2024، إلى جانب إمكانية الوصول إلى المنشور المشترك لمدة 17 ساعة، دليل على خطورة واقعة التزييف العميق [12] . وعلى المستوى المجتمعي، يؤدي انتشار تقنية التزييف العميق إلى تفاقم انتشار المعلومات المضللة من خلال السماح بتلفيق مقاطع فيديو ومقاطع صوتية واقعية مقنعة، والتي يُمكن نشرها على نطاق واسع عبر منصات الإنترنت المختلفة.

ومن خلال التزييف العميق، يُمكن تصوير الشخصيات العامة بشكل زائف وهي تشارك في أفعال لم ترتكبها أبدًا، مثل قبول الرشاوى، أو التعبير عن المشاعر العنصرية، أو الإدلاء بتصريحات حساسة دبلوماسيًا، أو إرتكاب أعمال عنف ضد المدنيين. ويُشكل تلفيق مقطع فيديو يصور الرئيس الأمريكي السابق باراك أوباما وهو يشير إلى ترامب باعتباره "غبيًا" مثالاً بارزًا لهذه الظاهرة، مما يؤدي إلى تأجيج الإرتباك، وتقويض الثقة العامة، وتفاقم الاستقطاب[13] . كما تُشكل عمليات التزييف العميق خطرًا كبيرًا على نزاهة العمليات الديمقراطية، حيث إنها تُمكن من إنشاء محتوى خادع مصمم لتضليل الناخبين، والتلاعُب بالتصورات العامة للمرشحين، وفي نهاية المطاف تقويض نزاهة وشرعية الإنتخابات. يفتح هذا الوضع بوابات التلاعب والدعاية، التي غالبًا ما يرتكبها المعارضون وحتى الكيانات الأجنبية. خلال الانتخابات الفرنسية في عام 2017، كانت حملة ماكرون ضحية لهجمات إلكترونية نُسبت إلى مجموعة قراصنة مدعومة من روسيا [14]. ولقد حذر وزير الداخلية البريطاني جيمس كليفرلي من عمليات التزييف العميق المدعومة من روسيا وإيران والتي تسعى إلى التلاعب بالعمليات الديمقراطية[15] يُظهر تورط كيانات أجنبية، أن مثل هذه الهجمات لا تهدد نزاهة الإنتخابات فحسب، بل لها أيضًا آثار عميقة على الأمن القومي. كما يثير ظهور تقنية التزييف العميق مخاوف بشأن قبول الأدلة في الإجراءات القانونية، حيث أن القدرة على إختلاق مواد سمعية وبصرية مقنعة تقوض موثوقية هذه الأدلة، مما قد يؤدي إلى أخطاء قضائية وتقويض سيادة القانون. وأخيرًا، يهدد الانتشار الواسع النطاق للتزييف العميق بتآكل ثقة الجمهور في مصداقية المعلومات، حيث يُصبح الأفراد مشككين بشكل متزايد في الأدلة البصرية والسمعية، مما يقوض أساس الخطاب وصنع القرار في المجتمع[16].كما ان الاستخدام غير المشروع لـــ Deepfake يتسبب في العديد من الإنتهاكات غير المشروعة التي تصيب المصالح المحمية قانونًا بالضرر أو الخطر والتي تتراوح من جرائم الاحتيال إلى جرائم إنتهاك الحقوق الشخصية. في 28 نيسان 2022، نشر مختبر الإبتكار التابع لليوروبول *Europol's Innovation Lab* تقريره الأول الذي قدّم نظرة عامة مفصلة عن الإستخدام الإجرامي لتقنية التزييف العميق. الذي عّد ظاهرة التزييف العميق نوعًا من الوسائط الإصطناعية التي يتم نشرها في الغالب بنية خبيثة "*Malicious Intent*"، على الرغم من أنها تُستخدم الآن غالبًا في التطبيقات الإيجابية ، تشير الوسائط الإصطناعية إلى الوسائط التي يتم إنشاؤها أو التلاعب بها باستخدام الذكاء الإصطناعي (AI). في معظم الحالات، يتم إنشاء الوسائط الإصطناعية للألعاب الإلكترونية، أو لتحسين الخدمات أو لتحسين نوعية الحياة، ولكن الزيادة في الوسائط

الإصطناعية والتكنولوجيا المحسنة، أدت إلى ظهور إمكانيات التضليل، بما في ذلك التزييفات العميقة. أن الافراد الذين يتمتنعون بالميول الإجرامية عادة مايكونون من أوائل المتبنين للتقنيات الجديدة. ونتيجة لذلك، فإنهم دائمًا ما يكونون متقدمين بخطوة واحدة على جهات إنفاذ القانون في تنفيذهم واستخدامهم وتكييفهم لهذه التقنيات. إن التوافر المتزايد للمعلومات المضللة والتزييف العميق سيكون له تأثير عميق في الطريقة التي ينظُر بها الناس إلى السلطة ووسائل الإعلام. ومع تزايد حجم التزييف العميق، يتم تقويض الثقة في السلطات والحقائق الرسمية. ويخشى الخبراء أن يؤدي هذا إلى وضع حيث لم يعد للمواطنين واقع مشترك، أو قد يخلق ارباكًا مجتمعيًا حول مصادر المعلومات التي يُمكن الإعتماد عليها؛ وهو الوضع الذي يُشار إليه أحيانًا بأسم "نهاية العالم المعلوماتي" أو "عدم الإكتراث بالواقع" *'Information Apocalypse' or 'Reality Apathy'* وهذا يجعل من الضروري أن نكون على دراية بهذا التلاعب وأن نكون مستعدين للتعامل مع الظاهرة، من أجل التمييز بين الاستخدام المشروع وغير المشروع لهذه التكنولوجيا. أما دور تقنية التزييف العميق وتأثيرها في الجرائم ، فأنها يُمكن أن تُسهل أنشطة إجرامية مختلفة، بما في ذلك: مضايقة أو إذلال الأفراد عبر الإنترنت؛ إرتكاب الإبتزاز والإحتيال؛ تسهيل الإحتيال في الوثائق؛ تزوير الهويات عبر الإنترنت وخداع آليات "اعرف عميلك"، المواد الإباحية غير الموافقة عليها؛ الإستغلال الجنسي للأطفال عبر الإنترنت؛ التزوير أو التلاعب بالأدلة الإلكترونية للتحقيقات في العدالة الجنائية؛ تعطيل الأسواق المالية؛ توزيع معلومات مضللة والتلاعب بالرأي العام؛ دعم روايات الجماعات المتطرفة أو الإرهابية؛ تأجيج الاضطرابات الاجتماعية والاستقطاب السياسي[17] وغيرها.

المطلب الثالث: سمات الجرائم المرتكبة بتقنية التزييف العميق.

The Third Requirement: Characteristics of Crimes Committed Using DeePfake Technology.

يعد التزييف العميق، وسيلة تعتمد على الذكاء الإصطناعي من أجل تحقيق أهداف محددة، سواء كانت هذه الاهداف إيجابية أو سلبية، وذلك بناءً على نوايا مستخدمي هذه التقنية. ان التزييف العميق كوسيلة، يمكن أن يُستخدم في مجموعة واسعة من السيناريوهات التي تتراوح بين الإبتكار والإبداع إلى الجرائم والتضليل بالرأي العام. من جانب آخر، تكاد تتاشبه سمات الجرائم المرتكبة عبر تقنية التزييف العميق على الرغم من اختلافها في المصلحة التي تعتدي عليها أو تُسبب الخطر لها، والتي يُمكن سوقها كالآتي: تتابع النشاط، العلانية، صعوبة مسائلة أو تتبع الجناة.

الفرع الاول: تتابع النشاط

First Branch: Activity Sequence

أن الفعل أو النشاط يُمثل أحد عناصر الركن المادي لأي جريمة. وفي جرائم التزييف العميق التي تعتمد على التلاعب بمقاطع الفيديو، الصوت والصورة باستخدام الذكاء الإصطناعي إذ يتم انتاج محتوى مزيف يبدو واقعيًا بشكل يصعب تمييزه، لذا تتمثل **المرحلة الاولى** بجمع ورصد صور – مقاطع فيديو – تسجيلات صوتيه للمجنى عليه (الضحية) ، ثم تبدأ **المرحلة الثانية** بتحريف تلك البيانات التي تم جمعها في المرحلة الأولى من أجل التلاعب بها وإنشاء المحتوى المزيف. أن مجرد جمع البيانات المتاحة والمباحة للجميع التي تنشرها الشخصيات العامة – الفنانين أو الأفراد الذين تنازلوا عن خصوصياتهم بإرادتهم على الشبكة المعلوماتية لايكون سببًا للتجريم مالم تكنْ تلك البيانات محمية ومؤمنه من قبل مالكها. لذا قيام الأشخاص بالتعدي عليها يعّد انتهاكًا للخصوصية الموجب للعقاب. ومن جانب آخر، أن مجرد إصطناع محتوى مزيف لايمس الشخص بصورة مستقلة لا يُمثل فعلًا خطيرًا يرقى الى التجريم [18]. فضلًا عن أنه توجد غاية بين هذين النشاطين، نشاط جمع البيانات ونشاط تزييفها بصورة مخالفة للواقع من أجل معالجتها بواسطة خورزميات معدة لهذا الغرض وإنتاج المحتوى المزيف. من ناحية أخرى، يتحقق التعدد المادي في هذه الجرائم، عندما يرتكب الجاني افعال مادية منفصلة باستخدام تقنية التزييف العميق، فتكون كل جريمة مادية قائمة بذاتها، الا انها يمكن أن تكون مرتبطة بجرائم أخرى[19]. وان هذا التعدد قد يكون تعدد في الضحايا (يتحقق عندما يكون المحتوى المزيف يمس مصلحة محمية لأكثر من شخص) او تعدد في الافعال الجرمية (تتحقق عندما يكّون المحتوى المزييف اكثر من فعل جرمي كالتشهير – إنتهاك الخصوصية- سرقة البيانات الشخصية[20]) أو تعدد المحتويات المزيفة (تتحقق عندما ينتج الجاني المحتوى كالصور – الفديو الذي يؤدي لجرائم متعددة) فضلا عن التكرار الزمني لذات الافعال الجرمية.

الفرع الثاني: العلانية

The Second Branch: Publicity

تتمثل العلانية[21] في جرائم التزييف العميق في تعريض الجاني للجمهور بصورة متعمدة للمحتوى المزيف الذي تم إصطناعه من قبله والذي يكون مخالفًا للحقيقة وشديد الإقناع بنفس الوقت، والذي يبذل الجاني جهده في إتقانه ليصعُب كشفه بإستخدام الأساليب التقليدية. ان الغرض من إنشاء المحتوى المزيف، اما يكون لغرض الإنتقام الإباحي – الإبتزاز – تشويه السمعة السياسية والتشهير وغيرها ،إذ لا فائدة تُرجى من قيام الجاني بصنع المحتوى المزيف دون إعلانه للغير. وغالبًا ما تُستخدم [22]المواقع

الإلكترونية أو مواقع التواصل الإجتماعي على اختلافها في ان تكون البيئة الخصبة أو الميدان الذي ينشُر بها الجاني محتواه وبالتالي، يُسهم هذا في إنتشار المعلومات الخاطئة على نطاق واسع، مما قد يُعرّض الأشخاص أو حتى الجهات الحكومية إلى مشاكل خطيرة، لاسيما إذا كانت هذه المحتويات المزيفة موجهة لتشويه السمعة أو التضليل في مواضيع مختلفة منها، سياسية أو اجتماعية حساسة. والجدير بالذكر، ان العلانية تتحقق حتى بعد إنتاج المحتوى المزيف بفترة زمنية فلا يتطلب وجود التعاصر الزمني بين إصطناع المحتوى ونشره في المواقع الإلكترونية او مواقع التواصل الإجتماعي حتى تتحقق العلانية، لذا فالعلانية يُمكن عدّها ركنًا في جرائم التزييف العميق[23].

الفرع الثالث: صعوبة مسائلة وتتبع الجناة.
The Third Branch: The Difficulty of Questioning and Tracking down the Perpetrators.

تتمثل صعوبة مسائلة الجناة في جرائم التزييف العميق في تحديد الجاني مرتكب الجريمة واسنادها له[24]. وتكمن هذه الصعوبة الى عوامل مختلفة منها: يستخدم الجناة تقنيات متقدمة تعتمد على الذكاء الإصطناعي وتقنيات الشبكات العصبية التوليدية، وتساهم هذه التقنية في إظهار المحتوى بدقة عالية من الواقعية ويصعب تمييزها عن المحتويات الحقيقية، وإخفاء هوية المجرمين باستخدام تقنيات الإخفاء كبرامج التشفير أو Vpn أو نشر المحتويات على مواقع الإنترنت المظلم Dark Web أو عن طريق الحسابات المجهولة [25]، سهولة انتشار التقنية مع توفر ادوات التزييف عبر الإنترنت دون الحاجة لمهارات متقدمة ، فضلًا عن صعوبة تطور التقنيات الحالية للكشف عن المحتويات المزيفة بسهولة. إذ أن أدوات التزييف أصبحت أمكانياتها متقدمة بصورة تصبح تكنولوجيا الكشف عنها قاصرة لمواكبة تطورها[26]. وفي ضوء ما قيل، تُطرح أسئلة حول تحديد المسؤول جزائيًا عن واقعة التزييف العميق، هل المسؤول جزائيًا مُنشئ المحتوى المزيف؟ أو من قام بتحميله على الموقع الالكتروني ؟ أو الذي شاركه عبر الإنترنت ؟ أم مزود الخدمة الذي علم بهذا المحتوى غير المشروع؟ للإجابة عن هذه التساؤلات، فلا تثور الصعوبة في تحديد المسؤول إذا كان الجاني من قام بكافة الإفعال السابقة فيكون الفاعل الذي إرتكب الركن المادي للجريمة برمته ، ولكن تصُعب المسألة اذا تعدد المساهمون في مراحل إرتكاب الجريمة فمن يكون الفاعل أو الشريك؟ وطالما أن هذه الجريمة الكترونية فتتسم بصعوبة الملاحقة الجزائية كونها تتسم بطابع عالمي وعابرة للحدود، فقد تُرتكب في اقليم دولة وتتحقق نتيجتها في أقليم آخر، لذا الأمر يستدعي تعاون الدول فيما بينها تجنبًا لافلات الجناة من قبضة العدالة[27].

المطلب الرابع: التزييف العميق تهديد إجرامي.
Fourth Requirement: Deepfake is a Criminal Threat.

أن التهديدات الإجرامية التي تنشأ باستخدام تقنية التزييف العميق تتنوع، فبعضها[28] يُصيب مصالح الأفراد والمؤسسات الخاصة، والأخر يُصيب مصالح المجتمع والدولة، لذا سنحاول التركيز على أبرز التهديدات الإجرامية التي تنشأ عن تقنية التزييف العميق والتي تصيب المصالح اعلاه ومنها:

الفرع الاول: التضليل والأخبار الكاذبة
First Branch: Misinformation and Disinformation

التضليل والأخبار الكاذبة معروفة عمومًا بـــ‘Fake News’"الأخبار الكاذبة". لقد حفزت الثورة التكنولوجية ظاهرة التضليل والأخبار الكاذبة، كما ويساهم الأستخدام المتكرر على نحو متزايد لوسائل التواصل الإجتماعي في كمية البيانات التي تتم مشاركتها ومعالجتها بواسطة الخوارزميات، وبها غيرت الطريقة التي يتم بها إنشاء الأخبار ونشرها. أن التضليل Misinformation يعني مشاركة معلومات غير صحيحة في حين أن الأخبار الكاذبة Disinformation يعني مشاركة معلومات غير صحيحة Malicious Intent بنية خبيثة. يُمكن أن يأخذ التضليل والأخبار الكاذبة أشكالًا عديدة مثل: المحتوى المنسوب بشكل خاطئ والمواقع الإلكترونية والأخبار المزيفة أو المستنسخة، كما يشمل أيضًا الصور ومقاطع الفيديو المعدلة والمختلقة (تسمى أيضًا التزييف العميق). ان المعلومات المضللة والمغلوطة تعمل على تضخيم التمييز والتحيز البشري، مما يؤثر سلبًا في الأقليات التي تتعرض بالفعل للتمييز، كما يمكن للروبوتات والمتصيدين وغيرهم من وكلاء الذكاء الإصطناعي زيادة نطاق حملات التضليل والأخبار الكاذبة إذ تعمل الخوارزميات التي تُنشئ فقاعات التصفية على تكثيف تأثيرها في المستخدمين بشكل كبير. كما إن حملات التضليل والأخبار الكاذبة تهدد العديد من حقوق الإنسان. فهي تعرض الديمقراطية[29] للخطر وتضع الصحفيين ونشطاء حقوق الإنسان في خطر[30]. كما تساهم الاخبار الكاذبة والتضليل بتقنية التزييف العميق على خطاب الكراهية أو التحريض على الكراهية، وتبرير وترويج نشر رسائل الكراهية القائمة على التعصب والعنصرية والعنف كما ويتعزز هذا بحقيقة أن الفضاء الرقمي يوفر إمكانية النشر بشكل مجهول، مما يؤدي إلى عدم المساءلة. وفي الوقت نفسه، فإن العديد من الاستجابات التي وضعتها الشركات والدول تهدد حرية التعبير على قدم المساواة[31].

الفرع الثاني: الانتقام الاباحي العميق
Second Branch: Deepfake Revenge Porn

التزييف العميق والانتقام الاباحي[32] يعدان من القضايا التي أثارت أهتمامًا كبيرًا في السنوات ألاخيرة. يعد الانتقام الاباحي العميق نوع من الانتقام الإباحي يستخدم تقنية التزييف العميق من أجل انشاء مقاطع فيديو أو صور إباحية مزيفة من اجل بثها أو مشاركتها لاشخاص (ذكر- أنثى) دون موافقتهم وبغرض الإنتقام[33]. كانت أول حالة أستخدام لشبكات GANs هي إنشاء مقاطع فيديو جنسية مزيفة؛ وبشكل خاص، مقاطع إباحية إنتقامية ومقاطع مزيفة لمشاهير. تُشير مقاطع الإباحية الإنتقامية إلى المواد الجنسية الصريحة التي يتم إنشاؤها ونشرها على نطاق واسع لإذلال أو تهديد أو إلحاق الأذى بشخص قطع العلاقة الحميمية. في الآونة الأخيرة، توسعت مقاطع الإباحية الإنتقامية لتشمل مقاطع فيديو جنسية مزيفة مماثلة حيث يتم توزيع مقاطع إباحية مزيفة غير موافقة من قبل قراصنة أو أي شخص يسعى إلى تحقيق مكاسب مالية أو شهرة بدلاً من الإنتقام للعلاقات المفقودة بشكل مباشر مع الشريك . تُشير فئة أخرى من محتوى الجنس المزيف العميق إلى مقاطع إباحية للمشاهير مع تبديل الوجوه إذ يتم فرض صور المشاهير على أجساد الأفراد المنخرطين في أعمال جنسية ، من ناحية أخرى، أن طبيعة الإنتقام الإباحي العميق تختلف عن طبيعة الإنتقام الإباحي المجرد، إذ أن الأخير يتمثل بإفشاء المقاطع أوالصور الجنسية وبثها بدون رغبة الشريك (المجني عليه)، فالواقعة هنا تعد حقيقية ورضائية وسرية ثم أعلنها الجاني بهدف الإنتقام وبدون رضى من الذي وقع عليه الفعل. وأن هذا الإنتقام يكون عادة بعد علاقة حميمية رضائية سابقة مشروعة كانت أم غير مشروعة بين المُجنى عليه والجاني الذي قام بالنشر دون علم المُجنى عليه، أو قد يكون الجاني أنتهك بيانات المُجنى عليه الشخصية (هاتف ذكي- جهاز كمبيوتر – بريد الكتروني) وقام بسرقة المحتويات الجنسية للضحية ونشرها على الأنترنت، في حين أن الواقعة الأولى تعد مزيفة وملفقة بصورة كاملة وتكون أشد خطورة من الإنتقام الإباحي المجرد، كون الجاني لم يرتكبْ الأفعال المزيفة من حيث الأصل، ولكن بفضل تقنيات الذكاء الإصطناعي تم أستخدام صوت وصورة وحركات وتعابير المُجنى عليه لإنتاج مقاطع فيديوية أو صور جنسية على وجه مخالف للحقيقية[34].

ومع ذلك، يمكن لأي شخص أن يكون ضحية لفرض وجهه على أجساد نجوم الإباحية المنخرطين في أعمال جنسية. من منظور أخلاقي ومعياري، يُنظر إلى مقاطع الفيديو الجنسية المزيفة العميقة في المقام الأول على أنها شكل جديد من أشكال انتهاك الخصوصية الجنسية. تخدم الخصوصية الجنسية وظيفة لا تقدر بثمن في المجتمع: فهي

تُسهل تطوير الهوية والحميمية والمساواة. وعلاوة على ذلك، تُشكل الخصوصية الجنسية أحد الركائز الأساسية للمنظومة البشرية واستقلالها. ومقاطع الفيديو الجنسية المزيفة العميقة لها تداعيات سلبية إضافية. على وجه الخصوص، يمكن أن تكون المواد الإباحية الإنتقامية في كثير من الأحيان جانبًا من جوانب الإذلال الجنسي والاستغلال، أو الإساءة الجسدية أو العقلية أو المالية للأفراد[35]. يمكن أيضًا مشاهدة المواد الإباحية الإنتقامية ومقاطع الفيديو الجنسية المزيفة العميقة في الشركات كأداة للاستغلال الجنسي أو التمييز في مكان العمل. إن انتهاك القيم الأخلاقية والقانونية المذكورة أعلاه، هو حجة قوية لمعالجة المواد الإباحية المزيفة العميقة عن طريق أدوات القانون العام، وخاصة القوانين الجنائية والإدارية. ونظرًا للطبيعة التكنولوجية للمواد الإباحية المزيفة العميقة[36]، فقد تنشأ ثلاث تحديات رئيسية في الممارسة القانونية. **التحدي الاول**: قد يكون من الصعب تحديد هوية الضحية. على عكس مقاطع الفيديو الإباحية، فإن المواد الإباحية المزيفة العميقة تتضمن المواد الإباحية ثلاثة أفراد (وليس اثنين): الشخص (الأشخاص) الذي يتم تمثيل جسده بصدق والشخص الذي تمت إضافة وجهه بواسطة الذكاء الإصطناعي. في كلتا الحالتين، لم يوافق أي من الأفراد المعنيين؛ وبالتالي يُمكن لكليهما رفع مطالبات فيما يتعلق بإنتهاك حقوق الصورة الذاتية. في الولايات القضائية حيث يتم حماية المواد الإباحية بموجب حقوق الطبع والنشر، يجوز لمؤلفي الفيلم رفع مطالبات تتعلق بتعديل الفيديو.

التحدي الثاني[37] يتعلق بتحديد هوية الجاني: هل هو الشخص الذي أنشأ الفيديو الأصلي، أو أنشأ مقطعًا مزيفًا عميقًا، أو قام بتحميله إلى الموقع وتوزيعه عبر الإنترنت؟ قد تختلف المواقف إعتمادًا على ما إذا كان الشخص الذي أنشأ الفيديو الأصلي والمزيف العميق والشخص الذي قام بتحميل وتوزيع المقطع المزيف العميق ليس هو نفسه. علاوة على ذلك، من المرجح أن يزعم المدعى عليه المحتمل أنه لا يمكن مقاضاة شخص ما لكشفه عن التفاصيل الحميمية لحياة شخص ما عندما لا تكون الحياة الشخصية لهذا الشخص هي التي يتم الكشف عنها في الواقع. **التحدي الثالثً**: قد يكون من الصعب فرض المسؤولية عن إنشاء وتوزيع وتخزين محتوى جنسي مزيف عميق، فقد لا تكون المنصات عبر الإنترنت التي تستضيف مثل هذا المحتوى قادرة أو راغبة في الإستجابة لطلبات إزالة المحتوى. فهل يجب أن يكون أمر المحكمة ضروريًا بالازالة؟ كما قد يواجه المدعي أيضًا عقبات قضائية وإختيار القانون المناسب الذي يتلائم الواقعة التي تعرض لها لاسيما في حالة عدم وجود نصوص قانونية كافية [38].

يمكن القول إن المواد الإباحية الإنتقامية هي أسوأ أشكال التزييف العميق، لأنها تنطوي على محتوى صريح دون موافقة الضحية وتخلق النتيجة الأكثر إذلالًا. لم

يكن رد الفعل الاجتماعي على محتوى الجنس المزيف العميق عدائيًا للغاية. فيما يتعلق بالإباحية الإنتقامية، قد يزعم البعض أن الضحية كان يجب أن لا يسمح بتصوير مقطع فيديو عاري في المقام الأول. بشكل عام، على الرغم من أن المواد الإباحية المزيفة العميقة تنتهك الخصوصية ويمكن عدها انتهاكًا للسياسة العامة وغير أخلاقية، إلا أن عددًا كبيرًا من مجتمع الإنترنت غير مبالٍ إلى حد ما. يمكن تفسير ذلك عن طريق العديد من الأفكار السلوكية. أولاً، يعاني الناس من تحيز المعلومات أو التأكيد، مما يشير إلى أنه طالما حصل الفرد على بعض المتعة ولم يكن هناك تهديد لحقوقه الشخصية أو ممتلكاته أو سمعته، فإن الفرد ليس ضدهم. ثانيًا، في حالة تزوير المشاهير، يرى الناس ما يريدون أن يكون صحيحًا، أي المشاهير وليس الشخص الذي يتم فرض وجه المشاهير على وجهه (تحيز الرغبة)[39]

الفرع الثالث: التزييف العميق في الحملات الإنتخابية.
Third Branch: Deep Forgery in Election Campaigns.

في الوقت الحاضر، يُشكل التزييف العميق تهديدًا خطيرًا على الحملات الإنتخابية Campaign Political حول العالم، إذ يُمكن استغلاله لإنتاج مقاطع فيديو أو تسجيلات صوتيه مزيفه تهدف إلى التضليل، والتأثير في الناخبين بطرق غير أخلاقية، وبالتالي تزرع الشكك في عقول الناخبين، فضلًا عن إحداثها فوضى سياسية تؤثر في نزاهة العملية الإنتخابية. ويُثار تساؤل حول كيفية أستخدام التزييف العميق في الحملات الإنتخابية؟ يُستخدم التزييف العميق في الحملات الإنتخابية عن طريق **التشهير السياسي الذي** يتمثل في إنتاج مقاطع مزيفة تُظهر مرشحين يتحدثون أو يقومون بتصرفات لاتمت لأي صلة بالواقع، مما يُسهم بإضعاف الثقة بالمرشحين من قبل قبل الناخبين[40].

التلاعب بالمواقف السياسية: إذ يتم إنشاء محتوى يبدو وكأنه حقيقي يُعبر عن مواقف معينة للمرشحين من أجل إحداث إنطباع خاطئ لدى فئة الناخبين يُظهر بأن المرشح يدعم أو يعارض قضية معينة وذلك بهدف التأثير في أصوات الناخبين مما يُرد سلبًا على نزاهة العملية الإنتخابية[41].

نشر الداعاية الزائفة بسرعة وإنتشار واسع: تُساعد مواقع التواصل الإجتماعي في المساهمة في نشر مقاطع الفيديو والصور المزيفة وحتى الحقيقية بسرعة البرق، وهذا يُسبب خطرًا كبيرًا يُصيب العملية الإنتخابية، خصوصًا إن أزالة المحتوى المزيف قبل أن يؤثر بصورة فعلية في الرأي العام يُشكل صعوبة. أن هذه الدعايات تسهم في احداث إنقسامات إجتماعية، فضلا عن زيادة التوترات بين مختلف الجماعات والتشكيك في

مصداقية المؤسسات السياسية والأعلامية[42]. وكذلك **المعلومات المضللة حول الإنتخابات عن طريق برامج الدردشة الآلية،** أقترح المشرعون في الولايات المتحدة الأمريكية، مشاريع قوانين بشأن أستخدام الذكاء الإصطناعي والإفصاح عنه فيما يتعلق ببرامج الدردشة الآلية في السياق الإنتخابي. حتى الآن، لم يتم تمرير مثل هذه المشاريع على مستوى الولاية أو المستوى الفيدرالي. أقترح المشرعون في العديد من الولايات المتحدة متطلبات للإفصاح عندما يتفاعل الأشخاص مع برامج الدردشة الآلية، والتي تُعرف على أنها حساب آلي عبر الإنترنت إذ يتم إنشاء جميع المنشورات أو معظمها بواسطة الذكاء الإصطناعي. أقترح مشروع قانون في ولاية نيويورك، شرطًا للإفصاح على وجه التحديد "لأي إتصال سياسي، سواء تم عن طريق مكالمة هاتفية أو بريد إلكتروني أو أي إتصال آخر قائم على الرسائل، والذي يستخدم نظام ذكاء إصطناعي للإنخراط في محادثة تشبه الإنسان".

تهدف مقترحات أخرى إلى تنظيم برامج الدردشة الآلية على نطاق أوسع، بما في ذلك مشروع قانون آخر في نيويورك كان من شأنه أن يتطلب من أي "مالك أو مرخص أو مشغل لنظام ذكاء إصطناعي توليدي("وهو الذكاء القادر على إنشاء نصوص أو صور أو وسائط أخريات باستخدام النماذج المولِّدة أو التوليدية.") "عرض تحذير واضح" للمستخدمين بأن النظام قد يكون غير دقيق أو غير مناسب. وعلى نحو مماثل، كان مشروع قانون في ولاية كاليفورنيا، يتطلب الإفصاح عن المعلومات في جميع الواجهات (البصرية والصوتية)، فضلاً عن "الموافقة الإيجابية" في بداية المحادثة. وكان مشروع قانون آخر في ولاية إلينوي يحظر أيضاً أستخدام الروبوتات في غياب الإفصاح، سواء في المعاملات التجارية أو أستخدام الروبوت "للتأثير في التصويت في الإنتخابات"[43]. على المستوى الفيدرالي، يتطلب قانون تصنيف الذكاء الأصطناعي لعام AI Labeling Act of 2023 [44] الذي يحظى بدعم الحزبين من مطوري الذكاء الإصطناعي التوليدي تضمين إشعار "واضح وجليّ "Clear and abvious" يُحدد أنظمة الذكاء الإصطناعي، بما في ذلك برامج الدردشة الآلية، على أنها تنتج محتوى تم إنشاؤه بواسطة الذكاء الإصطناعي. في حين، لا يقتصر أستخدام مشروع القانون على السياق الإنتخابي، فإنه ينطبق على برامج الدردشة الآلية في الإتصالات السياسية. وكذلك سعت بعض الولايات على تنظيم المكالمات الألية[45].

المبحث الثاني: مدى كفاية الأُطر القانونية والتقنية في مواجهة جرائم تقنية التزييف العميق.

The Second Topic: The Adequacy of Legal and Technical Frameworks to Confront Deepfake Technology Crimes.

لاتزال قوانين التزييف العميق في تطور او متأخرة في تشريعات الدول، لذا تكون المواجهة القانونية في الأساس تعتمد على تطويع القوانين التقليدية السارية المفعول وتكييفها من أجل مكافحة الجرائم المستحدثة التي تظهر بفعل تطور الحياة والوقاية منها. في حين تتجه بعض الدول إلى سنّ تشريعات جديدة لمكافحة هذه الظواهر خصوصًا بعد فشل القوانين التقليدية في مواجهتها، وقد ثبت قبل عدة عقود ولاسيما في ثمانينات القرن السابق، عدم كفاية أو فاعلية القوانين التقليدية لمواجهة أو مكافحة الجرائم السيبرانية[46] ، لذا لجأ المشرع في مختلف دول العالم إلى سنّ قوانين متخصصة مع الجرائم المستحدثة التي ترافق التطور التكنولوجي الذي تشهده البشرية، الا أنه يبقى سؤال يتبادر إلى الأذهان هو، ما مدى كفاية القوانين في مواجهة جرائم تقنية التزييف العميق؟ وللإجابة على السؤال سنقسم هذا المبحث على أربعة مطالب وعلى النحو الآتي:-

المطلب الأول: الأُطر القانونية لمواجهة جرائم تقنية التزييف العميق في قارة آسيا[47] "جمهورية الصين الشعبية انموذجًا".

First Requirement: Legal Frameworks to Combat Deepfake Technology Crimes in Asia “The People’s Republic of China ”as a Model.

تعُد جمهورية الصين الشعبية، من أوائل الدول التي أصدرت مجموعة من التشريعات والأحكام التي نظمت الذكاء الإصطناعي بوجه عام وتقنية التزييف العميق بوجه خاص. كما أتخذت موقفًا صارمًا من تجريم التزييف العميق. في نهاية العام 2022 أصدرت إدارة الآمن المعلوماتي بالتعاون مع وزارة الصناعة والتكنولوجيا ووزارة الآمن العام الصيني نظامًا تحت عنوان ،" أحكام إدارة خدمات معلومات الإنترنت للتزييف العميق[48] Provisions on the Administration of Deep Synthesis Internet Information Services” هذه الأحكام تألفت من (25) مادة تتعلق باستخدام تقنية التزييف العميق. فقد أشارت المادة (6) منه بقولها، " لا يجوز لأي منظمة أو فرد أستخدام خدمات التزييف العميق لإنتاج أو إعادة إنتاج أو نشر أو نقل معلومات محظورة بموجب القوانين أو اللوائح الإدارية، أو الانخراط في أنشطة محظورة بموجب القوانين واللوائح الإدارية مثل تلك التي تعرض الأمن القومي والمصالح للخطر، أو تضر بصورة الأمة، أو تضر بالمصلحة العامة للمجتمع، أو

تعكر صفو النظام الإقتصادي أو الإجتماعي، أو تضر بالحقوق والمصالح المشروعة للآخرين،" وبموجب النظام ،" لا يجوز لمقدمي ومستخدمي خدمات التزييف العميق أستخدام خدمات التزييف العميق لإنتاج أو إعادة إنتاج أو نشر أو نقل معلومات إخبارية مزيفة. وفي حالة إعادة طباعة المعلومات الإخبارية التي يتم إنتاجها ونشرها بناءً على خدمات التزييف العميق، يجب إعادة إنتاج المعلومات الإخبارية التي تنشرها وحدة المصدر لمعلومات الأخبار على الإنترنت وفقًا للقانون." كما فرض النظام جملة التزامات على عاتق مزود الخدمة على التزييف العميق منها، أمن البيانات، وحماية المعلومات الشخصية، ومنع الإحتيال في شبكات الإتصالات، والإستجابة للطوارئ، ويجب أن يكون لديهم تدابير وقائية تقنية آمنة وقابلة للتحكم وغيرها[49] ، كما يجب عليهم التحقق من معلومات الهوية الحقيقية لمستخدمي خدمات التزييف العميق وفقًا للقانون عن طريق وسائل مختلفة منها: أرقام الهواتف المحمولة، وأرقام بطاقات الهوية، وأكواد الإئتمان الإجتماعي الموحدة، أو خدمة التحقق من الهوية العامة عبر الإنترنت في المدينة، ويجب ألا يقدموا خدمات نشر المعلومات لمستخدمي خدمات التزييف العميق الذين لم يتم التحقق من معلومات الأسم الحقيقي لهم[50]، وعندما يكتشف مقدمو خدمات التزييف العميق معلومات غير قانونية أو سلبية، يجب عليهم استخدام التدابير لمعالجتها وفقًا للقانون، وتخزين السجلات ذات الصلة، وتقديم تقرير على الفور إلى إدارة الإتصالات أو الإدارات ذات الصلة المسؤولة؛ وإتخاذ التدابير وفقًا للقوانين والإتفاقيات ضد مستخدمي خدمة التزييف العميق ذات الصلة، مثل إعطاء التحذيرات، والوظائف المقيدة، وتعليق الخدمة، وإغلاق الحساب[51]، إبلاغ السلطات المختصة ، ووضع العلامة المائية[52] Watermark على المحتوى بشكل لا يعيق أستخدام التقنية[53]. على أنه بالرغم من أهمية هذا النظام والإهداف التي يناضل من أجل تحقيقها حتى ان بعض سياسي الولايات المتحدة أبدو تخوفهم من أن تصبح الصين وقوانيها في هذا المجال النموذج الأول لدول العالم، فإن هذا النظام يواجه تحديات وصعوبات كبيرة تتمثل بآلية التطبيق والغموض والصعوبة في تفسره، لذا تعرض لنقد شديد[54]. وعلى مستوى القوانين التقليدية في الصين، يعاقب قانون العقوبات الصيني لسنة 1997 في المادة (181) ، بالحبس كل من زيّف أونشر معلومات كاذبة بهدف التأثير السلبي في الأسواق والأسهم وإثارة الفوضى في سوق تداول الأسهم، أما المادة (221) ، فقد عاقبت بالحبس كل من يقوم بتزوير معلومات كاذبة ونشرها عبر الشبكات المعلوماتية أو مواقع التواصل الإجتماعي بقصد النيّل من النظام العام أو التشهير بالآخرين. وبناءً على ماسبق، يتضح أن المشرع الصيني أوجد أدوات قانونية رادعة في مجال مكافحة جرائم هذه التقنية من أجل التصدي لهذه الجريمة مع إعطاء الألولية للآمن المجتمعي

وسيطرة الحكومة على الأمن الرقمي بما يتناسب مع فلسفة النظام السياسي والأجتماعي للصين[55].

المطلب الثاني: الأُطر القانونية لمواجهة جرائم تقنية التزييف في قارة أمريكا الشمالية " الولايات المتحدة الأمريكية إنموذجًا".

Second Requirement: Legal Frameworks to Combat Deepfake Technology Crimes in North America "USA as a Model".

في الولايات المتحدة الأمريكية ، يتطور المشهد القانوني الذي يحيط بجرائم التزييف العميق، إذ تتخذ بعض الولايات والحكومة الفيدرالية خطوات لمعالجة القضايا التي تُثيرها هذه التكنولوجيا في أمريكا ، وسنسلط الضوء على منظُور القانون الفيدرالي والمنظُور القانوني للولايات من الجريمة وعلى النحو الآتي:-

الفرع الاول: منظُور القانون الفيدرالي Federal Law : First Branch : Perspectiveلم تشرعْ الولايات المتحدة الأمريكية على المستوى الفيدرالي الى يومنا هذا قانونًا شاملًا يستهدف جريمة التزييف العميق بشكل مباشر، ومع ذلك يُمكن تطبيق القوانين الحالية الفيدرالية مثل، قانون منع سرقة الهوية وإفتراضها **Identity Theft and Assumption Deterrence Act** [56] والذي يُعّد أحد القوانين المثيرة للإهتمام التي يُمكن أستخدامها في ظروف محددة للغاية عندما يتعلق الامر بالإحتيال، مثل مقطع فيديو مزيف أو تسجيل صوتي يطلب المال أو الوصول إلى حساب ، ومع ذلك، في حالات مثل حالة السيدة مارتن ,والتي كانت دعوى التشهير الوحيدة التي ذكرت صراحةً استخدام "التزييف العميق" مرفوعة في يونيو 2021. [57] والتي اشارت بها المحكمة حيث لا يوجد إحتيال فعلي، ولا تنطبق سرقة الهوية على القضية. إذا تم تفسير التزييف العميق الخبيث على أنه تهديد بموجب المادة (c) 875§ U.S.C. 18 والتي نصت على ، يدان ويحبس شخصًا لمدة عامين إذا كان الشخص الفقرة (1) ، يتعمد إجراء إتصال يحتوي على تهديد حقيقي بالإيذاء في التجارة بين الولايات أو التجارة الخارجية، والفقرة (2) يقصد أن يكون الاتصال تهديدًا حقيقيًا بإيذاء شخص آخر أو يعرف أن متلقي التهديد سيفهم أنه تهديد[58]. وكذلك قانون الإحتيال وإساءة استخدام الكمبيوتر Computer Fraud and Abuse Act [59] على بعض الجرائم التي تستخدم تقنية التزييف العميق.

ومع ذلك، في كثير من الحالات، قد يواجه المدعي العام مشكلة في إثبات أن التزييف العميق يُشكل تهديدًا حقيقيًا. ولعل الأداة الأكثر فعالية للمدعين العامين هي قوانين المطاردة الإلكترونية الفيدرالية 18 U.S.C. cyberstalking statutes

Federal، اذا تنطبق المادةA2261 § على السلوك الذي "يضع [الشخص] في خوف معقول من الموت، أو الإصابة الجسدية الخطيرة [...] (i) ذلك الشخص؛ (ii) أحد أفراد الأسرة المباشرين؛ أو (iii) الزوج أو الشريك الحميم لذلك الشخص ، كما يجب أن يكون لدى المدعى عليه النية الإجرامية لقتل أو إيذاء أو مضايقة أو ترهيب أو وضع [الضحية] تحت المراقبة. أن الملاحقات الجنائية لها ميزة كونها أكثر رادعًا من إمكانية المسؤولية المدنية وحدها، أن مثل هذه القوانين وحدها لا تحظر بوضوح ممارسة إنشاء مقاطع فيديو مزيفة خبيثة. في الأساس، لا تخضع أدلة مقاطع الفيديو المزيفة حاليًا لأي نهج إثباتي، والمعايير القانونية الحالية التي تحد من صحة الأدلة غير كافية. عند التعامل مع أدلة التزييف العميق في المحكمة[60]، يجب على القضاة والمحامين تجنب فخاخ الإثبات مع التعامل أيضًا مع شكوك الادعاء وعدم ثقته، تكمن المشكلة أيضًا في تحديد من أنشأ التزييف العميق - سواء تم إنشاؤه بواسطة الذكاء الاصطناعي أو البشر [61]. فضلا عن National Defense Authorization Act (NDAA) 2021 قانون تفويض الدفاع الوطني 2021، هذا القانون يوجه وزارة الأمن الداخلي U.S. Department of Defense إصدار تقرير سنوي للسنوات الخمس المقبلة حول التزييف العميق اعتبارا من تاريخ اصداره، والذي يجب أن يغطي جميع أشكال الضرر المحتمل من التكنولوجيا، بما في ذلك كل شيء من حملات التأثير الأجنبي إلى الاحتيال إلى الإضرار بفئات سكانية معينة. وقد أدى هذا إلى توسيع نطاق تقرير التزييف العميق الذي دعا إليه قانون الدفاع الوطني للعام الذي سبقه. بالإضافة إلى ذلك، يأمر القانون وزارة الأمن الداخلي بدراسة تقنية إنشاء التزييف العميق والحلول الممكنة للكشف والتخفيف عنه. أخيرًا، يتطلب القانون من وزارة الدفاع الأمريكية، دراسة إمكانية قيام الخصوم بإنشاء محتوى مزيف عميق يصور أفرادًا عسكريين أمريكيين أو عائلاتهم، والتوصية بتغييرات في السياسة. في أواخر ديسمبر 2020، وقع الرئيس الامريكي دونالد ترامب على قانون آخر، وهو قانون تحديد مخرجات الشبكات التنافسية التوليدية Identifying Outputs of Generative Adversarial Networks Act[62] . يتطلب هذا القانون من مؤسسة العلوم الوطنية البحث في تقنية التزييف العميق وتدابير الأصالة، ويتطلب من " National Institute of Standards and Technology"المعهد الوطني للمعايير والتكنولوجيا دعم تطوير المعايير المتعلقة بالتزييف العميق، ويوجه كلتا الهيئتين لتطوير طرق للعمل مع القطاع الخاص على قدرات تحديد الهوية باستخدام التزييف العميق[63].

في عام 2019 تم إقتراح قانون فيدرالي S. 2065, the Deepfake Report Act of 2019[64]، يشمل هذا القانون الطرق التي تُستخدم بها مقاطع الفيديو

المزيفة لإرتكاب الاحتيال، والتسبب في الضرر، وإنتهاك الحقوق المدنية الفيدرالية، ويوضح مدى تطبيق متطلبات قانون حرية المعلومات وقانون الحد من الأعمال الورقية. وقد تم تمرير التعديل والتشريع المعدل بالتصويت الجماعي بحضور أعضاء مجلس الشيوخ. في عام 2020 أقتراح قانون فيدرالي DEEP FAKES Accountability Act of 2020 للمسألة عن التزييف من أجل معالجة المخاوف المتزايدة حول إساءة أستخدام تقنية التزييف العميق لاسيما عند أستخدامه بشكل سيء لخداع الآخرين، وقد تضمن عدة محاور:

1. متطلبات العلامة المائية الرقمية Watermark: يُلزم مقترح القانون وضع علامات مائية رقمية[65] أو إعلانًا صوتيًا[66] ونصًا صريحًا مكتوبًا وإفصاحات[67] على جميع محتويات التزييف العميق لإعلام المشاهدين بأن المحتوى قد تم تغييره أو توليفه. وبخلافه يعد جريمة معاقب عليها بالغرامة او الحبس الذي لايزيد على خمس سنوات أو كلا العقوبتين[68] .

2- العقوبات المدنية: لقد أنشأ القانون عقوبة مدنية (تعويض مدني) قيمتها 150 ألف دولارعن كل فعل يُخالف أحكام المواد السابقة، فضلًا عن التعويض عن كل ضرر يسببه المحتوى المعدل. [69]

3- منسق مكاتب الإدعاء العام: المدعي العام الأمريكي ملزم استنادًا للقانون بتعين منسق في كل مكتب من مكاتب الأدعاء العام في كل ولاية أمريكية، تكون مهمته إستقبال الشكاوى من المواطنين حول أي محتوى مزيف متداول من إنتاج دولة أجنبية أو وكلائها . هذا المنسق يقوم بمتابعة الإجراءات القضائية ضد تلك الجهة. [70]

4- يلزم هذا القانون الشركات التكنولوجية الأمريكية التي تنتج تقنية التزييف العميق، أن يكون من ضمن خصائص التطبيق أو التقنية تضمينها العلامة المائية ومعلومات حول شروط الأستعمال وبيان المسؤولية القانونية (الجزائية والمدنية) الواردة في القانون[71].

5- هذا القانون يدعو إلى إنشاء قوة تنفيذية لدى وزارة الأمن الداخلي لكشف ومكافحة التزييف العميق[72].

الفرع الثاني: المنظُور القانوني للولايات
: Second Branch : States Law Perspective

في ظل طفرة الذكاء الإصطناعي إرتفعت التشريعات الأمريكية التي تهدف إلى تنظيم هذه التكنولوجيا الجديدة. يتم التعامل مع الجرائم الناشئة باستخدام تقنية التزييف العميق بالإعتماد على مجموعة قوانين منها قوانين جنائية، قوانين إنتهاك حقوق الطبع والنشر[73]- قوانين الحق في الدعاية [74]-قوانين التشهير[75]. في عام 2019، سنت ولايتان قوانين تجرم بعض أنواع التزييف العميق. أصبحت فيرجينيا أول ولاية في أمريكا تفرض عقوبات جنائية على توزيع المواد الإباحية المزيفة العميقة غير المقبولة[76]. جعل القانون *Virginia Revenge Porn Law (Amended to include deepfakes)* ، الذي دخل حيز التنفيذ في 1 يوليو 2019، توزيع الصور ومقاطع الفيديو الصريحة "المُنشأة بشكل زائف" غير المقبول جنحة من الدرجة الأولى، يعاقب عليها بالحبس لمدة تصل إلى عام وغرامة قدرها 2500 دولار.

وفي 1 سبتمبر 2019، أصبحت تكساس أول ولاية في البلاد تحظر إنشاء وتوزيع مقاطع فيديو مزيفة عميقة تهدف إلى إيذاء المرشحين لمناصب عامة أو التأثير في الإنتخابات. يعرّف قانون تكساس Texas Election Interference Law. "فيديو التزييف العميق" بأنه مقطع فيديو "تم إنشاؤه بقصد الخداع، ويبدو أنه يصور شخصًا حقيقيًا يقوم بعمل لم يحدثْ في الواقع". وهذا يجعل الأمر جنحة من الدرجة الأولى، يعاقب عليها بالحبس لمدة تصل إلى عام في سجن المقاطعة وغرامة قدرها 4000 دولار، لشخص "يُنشئ" مقطع فيديو مزيفًا عميقًا و"يتسبب" في "نشر أو توزيع هذا الفيديو في غضون 30 يومًا من الإنتخابات"، إذا فعل الشخص ذلك "بقصد إيذاء مرشح أو التأثير على نتيجة الانتخابات".

أصدرت كاليفورنيا[77] قانونين في أكتوبر 2019، يسمحان لضحايا المواد الإباحية المزيفة العميقة غير المقبولة بالمقاضاة عن الأضرار ومنح المرشحين لمناصب عامة القدرة على مقاضاة الأفراد أو المنظمات التي توزع "بسوء نية" مقاطع فيديو مزيفة عميقة متعلقة بالإنتخابات دون ملصقات تحذيرية بالقرب من يوم الانتخابات.[78] ، في الفترة الممتدة من 1 يناير الى 31 يوليو لعام 2024 سنت 14 ولاية قوانين أو أحكاما جديدة لتنظيم استخدام التزييف العيمق في الإتصالات السياسية فضلًا عن وجود سياسات جديدة متعلقة بالذكاء الإصطناعي ودورها في إدارة الإنتخابات وكيفية استخدامه لمهاجمة آمن الإنتخابات أو قمع الاصوات. مع إغلاق العديد من الهيئات التشريعية للولايات المتحدة لجلساتها في عام 2024 ، تم تقديم (151) مشروع قانون يتناول التزييف العميق والوسائط الخادعة في سياق الإنتخابات حتى هذا العام، وهذا

يُمثل مايقارب ربع جميع القوانين المقدمة حول موضوع الذكاء الإصطناعي . لقد استهدف مايقارب 100 مشروع "التزييف العميق والوسائط الخادعة الأخرى على الإتصالات السياسية للجمهور"[79] . تُمثل أحدى نقاط التمييز بين هذه القوانين هي ما إذا كانت تُحظر صراحة أستخدام التزييف العميق وغيرها من الوسائط التي تم التلاعب بها في الإتصالات السياسية أو ما إذا كانت تسمح بها طالما تم تصنيفها. وبالمثل ، في معظم الولايات، يدخل الحظر أو شرط الإفصاح حيز التنفيذ في وقت قبل الإنتخابات (عادة قبل 90 أو 120 يومًا من الإنتخابات)، بينما في بعض الولايات، لايوجد هذا الشرط. حتى الأن هذا العام(2024)، لم تسنّ الولايات سوى قوانين إفصاح جديدة بدلًا من الحظر الصريح [80]. بعض الولايات أصدرت قوانين بشأن **ترهيب الناخبين (Voter Suppression)**. لقد اصدرت ولاية ميسيسيبي ، مؤخرًا تشريعًا يجرم التوزيع المتعمد لـــ " الرقمنه Digitization" في غضون 90 يومًا من الأنتخابات والتي يتم نشرها بقصد إيذاء المرشح أو التأثير في نتائج الأنتخابات أو ردع أي شخص عن التصويت، وعرف القانون الرقمنه بأنها،" تغيير صورة أو صوت بطريقة واقعية باستخدام صورة أو صوت لشخص، بخلاف الشخص المصور، أو صور أو صوت تم إنشاؤها بواسطة الكمبيوتر، والتي تسمى التزييف العميق،" وتشمل كذلك إنشاء صورة – صوت عن طريق أستخدام البرامج أو التعلم الآلي للذكاء الأصطناعي أو أي وسيلة أُخرى يتم إنشاؤها بواسطة الكمبيوتر أو الوسائل التكنولوجية." وكذلك ولاية الينوي والتي سعت الى تحديث قوانين ترهيب الناخبين في الولاية وتعديل تعريف " الخداع أو التزويرDeception and Forgery" ليشمل انشاء وتوزيع محتوى مضلل على وسائل التواصل الإجتماعي، من المرجح أن يثني الناخبين إلا أنه لم يُمرر إلى هذا الوقت. كما سعت بعض الولايات إلى الحماية وبشكل إستباقي من **التهديدات التي يتعرض لها المسؤولون عن الإنتخابات والعاملون فيها** وذلك من أجل تعزيز وعي الناخبين عن طريق حظر أو تصنيف الوسائط الإجتماعية التي تضلل الناخبين بشأن سلوك المرشحين للمناصب السياسية ، إلا أنه لم يتم تمرير أي من هذه القوانين. على سبيل المثال، في كاليفورنيا، يُشير مشروعان قانونيان منفصلان إلى محتوى خادع يُظهر مسؤولاً إنتخابياً يفعل أو يقول شيئاً يتعلق بوظيفته "من المرجح بشكل معقول أن يقوض الثقة بشكل زائف في نتيجة واحدة أو أكثر من المسابقات الانتخابية". يمتد أحد مشاريع القوانين أيضًا إلى تقييد المحتوى الخادع ليشمل "آلة تصويت أو بطاقة اقتراع أو موقع تصويت أو ممتلكات أو معدات أخرى تتعلق بالإنتخابات في كاليفورنيا يتم تصويرها بطريقة زائفة بشكل مادي". وقد مُرر كلا المشروعين في جمعية كاليفورنيا وهما الآن في مجلس الشيوخ.

وبالمثل، اقترحت جورجيا مشروع قانون من شأنه أن يجرم "التدخل الإحتيالي في الإنتخابات "Fraudulent Election Interference" "نشر وسائل إعلام خادعة بشكل مادي في غضون 90 يومًا من الإنتخابات بقصد الخداع ... [وخلق] إرتباك حول إدارة مثل هذه الإنتخابات". ولدى نيوجيرسي إقتراح مماثل يُجرّم "الكشف عن علم أو بتهور عن وسائل إعلام سمعية أو بصرية خادعة بقصد خداع الناخب بمعلومات كاذبة عن المرشح أو السؤال العام أو الانتخابات" في غضون 90 يومًا من الانتخابات.[81]

المطلب الثالث:الأُطر القانونية لمواجهة جرائم تقنية التزييف العميق في قارة أوروبا، الإتحاد الآوروبي أنموذجًا".

The Third Requirement: Legal Frameworks to Confront Deepfake Technology Crimes in Europe, "The European Union as a Model".

على مستوى الإتحاد الأوروبي، لقد أُتخذ الإتحاد خطوات واضحة من أجل مكافحة التزييف العميق، وذلك لمخاطره على الخصوصية والآمن، ولقد طبق عدة أدوات وأُطر من أجل التصدي القانوني لهذه التقنيه سنحاول تسليط الضوء على أبرزها منها، **الاداة الاولى: قانون الذكاء الأصطناعي (Artificial Intelligence Act)** الذي يعد أول تشريع شامل في العالم وضُع من أجل تنظيم أستخدام الذكاء الإصطناعي، قدمته المفوضية الأوروبية في أبريل2021 ووافق وزراء الإتحاد الأوروبي عليه بشكل نهائي، في (21 مايو/أيار 2024)[82]. هذا القانون يهدف إلى وضع إطار قانوني لتنظيم تطوير وأستخدام أنظمة الذكاء الإصطناعي داخل الإتحاد الأوروبي وحماية حقوق الإنسان وتعزيز الشفافية والسلامة، مع ضمان الإستفادة من التقنيات الحديثة بشكل أخلاقي ومسؤول. هذا القانون صنف خطورة انظمة الذكاء الإصطناعي وفقًا لاربعة مستويات وعلى النحو التالي:-

المستوى الاول: الخطورة غير المقبولة في هذا المستوى تُشكل منتجات الذكاء الإصطناعي خطورة على (سلامة وعيش الأفراد والحقوق المكفولة لمواطني الإتحاد الأوروبي). وتأسيسيًا على ذلك، يُمنع التعامل أو إنتاج أو طرح أي من منتجات الذكاء الإصطناعي في دول الإتحاد التي تصنف ضمن بند الخطورة غير المقبولة.[83]

المستوى الثاني: الخطورة العالية إذ يتم إخضاع المنتجات الذكية لقواعد صارمة في التعامل، منها وجوب تسجيل المنتج في قاعدة البيانات الأوروبية ،"وتكون عالية الخطورة إذا كانت تُشكل، في ضوء الغرض المقصود منها، خطرًا كبيرًا على صحة وسلامة الأشخاص أو حقوقهم الأساسية، مع مراعاة شدة الضرر المحتمل واحتمال حدوثه، ويتم أستخدامها في عدد من المجالات المحددة مُسبقًا والمُحددة في هذه

اللائحة."[84] كالانظمة المستخدمة في إتخاذ قرارات التوظيف أو تشخيصات الرعاية الصحية.

المستوى الثالث: الخطورة المتوسطة أو المحدودة إذ تخضع منتجات الذكاء الإصطناعي لقوعد محددة، تقنيات التزييف العميق تقع من ضمنها. ووفقًا للمادة (52) فقرة (3) أُوجب على مستخدمي تقنيات التزييف العميق بالتصريح بحقيقة المحتوى المزيف مالم يكنْ الأستخدام لأغراض مشروعة تتعلق بكشف أو منع الجريمة أو التحقيق الجنائي ومحاكمة المجرمين ، مثالها تطبيقات الدردشة أو تطبيقات التفاعل مع العملاء.

المستوى الرابع : الخطورة الواطئة أو المنخفضة لاتخضعْ أي من منتجات الذكاء الأصطناعي لأي قيود. مثالها الألعاب الألكترونية أو الفلاتر التجميلية، فلا تتطلبْ وجود قانون صارم لتنظيمها، إلا أن هذا لايمنعْ من التزام هذه التطبيقات بمعايير الجودة والشفافية.

لقد حددت المادة (71)[85] العقوبات والغرامات في هذا القانون، فقد اشارت الفقرة (1) من المادة (71)، أنظمة الذكاء الإصطناعي عالية المخاطر: بالنسبة لمقدمي أنظمة الذكاء الإصطناعي عالية المخاطر الذين يفشلون في الأمتثال للإلتزامات، قد تصل الغرامات إلى 30 مليون يورو أو 6% من إجمالي المبيعات السنوية العالمية، أيهما أعلى." والفقرة (2) التوثيق غير الصحيح أو المضلل،"إذا قدم المزود أو المستخدم معلومات غير صحيحة أو غير كاملة أو مضللة في الوثائق، أو لم يضمنْ الشفافية للمستخدمين، فقد تصل الغرامات إلى 20 مليون يورو أو 4% من إجمالي المبيعات السنوية العالمية." وأخيرًا الفقرة (3) المخالفات الأخرى،"بالنسبة للمخالفات التي لا تندرج ضمن فئات المخاطر العالية، قد تصل الغرامات إلى 10 ملايين يورو أو 2% من إجمالي المبيعات السنوية العالمية، أيهما أعلى."

الاداة الثانية:اللائحة العامة لحماية البيانات General Data Protection Regulation (2016 GDPR) هذه اللائحة لها دور فعّال في التصدي لجرائم التزييف العميق عن طريق حماية خصوصية وبيانات الأفراد الشخصية عن طريق ضمان حقهم في التحكم في بياناتهم وتقر قيودًا صارمة على أستخدام أو جمع البيانات. وفقًا للمادة (5 و 6[86]) من اللائحة، فقد حددت المبادئ الأساسية الواجب إتباعها عند معالجة البيانات الشخصية ومنها "purpose limitation", "data minimization", "accuracy", "storage limitation", and "integrity and confidentiality". " الغرض من التقييد"، و"تقليل البيانات"، و"الدقة"، و"حد التخزين"، و"النزاهة والسرية". وأن تُستخدم للغرض التي تم جمعها لإجله فقط،

وبخلافه يُعد الجامع للبيانات لغرض التزييف العميق مخالفًا للمادة(5) من اللائحة (GDPR) وإذا كان الجمع بدون موافقة صريحة من قبل صاحب البيانات من أجل إنشاء المحتوى المزييف (المادة 6) ومنحت المادة (17) من اللائحة[87] ،" الحق في المسح أو النسيان A right to be forgotten " فللمتضرر من المحتوى المزييف حق طلب حذف هذا المحتوى من أي نظام/ منصة تستخدم بياناته بشكل غير قانوني [88] . كما أشارت المادة 82 من GDPR[89] أن أي شخص عانى من ضرر مادي أو غير مادي نتيجة لإنتهاك هذه اللائحة يحق له الحصول على تعويض من المتحكم أو المعالج عن الضرر الذي لحق به[90].كما فرضت المادة (83) عقوبة الغرامة التي تصل إلى 20 مليون يورو أو 4% من أجمالي الإيرادات المالية السنوية.

الاداة الثالثة: قانون الخدمات الرقمية 2022 (Digital Services Act - DSA)

هذا القانون تناول المحتوى غير القانوني والإعلانات الشفافة والتضليل ومن ضمنها المحتويات المزيفة، وهو يعمل على تحديث توجيه التجارة الإلكترونية لعام 2000 في قانون الإتحاد الأوروبي، وتركز بعض مواده على إلزام المنصات بإتخاذ إجراءات صارمة بشأن المحتوى غير القانوني أو المضلل، ولقد اشارت المادة(14) منه آلية إزالة المحتويات المزيفة وإستجابة المنصات بالرد بسرعة على بلاغات المستخدمين وإزلة المحتوى إذا أضر بالمصالح الخاصة أو العامة، والشفافية في الإعلانات في حالة إذا تم أستخدام الذكاء الإصطناعي بإنشأها وإعلام المستخدمين بها (المادة 30)، وفي حال عدم التزام مالكي المنصات بإحكام هذا القانون فتُفرض الغرامات التي قد تصل إلى 6% من إيرادات المنصة [91]. هذا وتوجد إداوت أُخرى منها قوانين مكافحة التضليل الإعلامي من أجل حماية الإعلام من المحتويات المزيفة في ضلّ التسارع الهائل لتكنولوجيا الذكاء الإصطناعي. ويطمح الإتحاد الأُوروبي بموجب الأدوات والأليات التي يستخدمها في التصدي لآثار التزييف العميق عن طريق إلزام المنصات بتطوير وسائل وأدوات تقنية من أجل مكافحة إنتشار المعلومات المزيفة، فضلا عن سعيه إلى تطوير التعاون الدولي مع دول ومنظمات أُخرى من أجل إيجاد معايير وتقنيات مشتركة جديدة من أجل التصدي لهذه التقنية. ويرى الباحث، أنه على الرغم من كثرة قوانين الدول التي تم بيان موقفها القانوني من جرائم هذه التقنية، فتبقى المخاوف من كيفية تنفيذ هذه القوانين لاسيما في حالة عدم الإمتثال في إزالة المحتويات المزيفة أو تجاهلها من قبل المنصات أو المؤسسات المعنية، والصعوبة الأُخرى تتمثل في مدى قدرة هذه القوانين مواكبة التطورات المتلاحقة لتقنية التزييف العميق وقدرتها على التكيف في ضلّ التسارع التكنولوجي للذكاء الإصطناعي.

بعد تناولنا للأُطر القانونية أعلاه، تبين أن الصين تبنت موقفًا صارمًا في تنظيم المحتوى على الإنترنت وقد شددت المسؤولية القانونية على الأفراد الذين يخالفون القوانين الصينية السالفة الذكر وإنشاء المحتوى المزيف أوأي تلاعب بالمعلومات وفرض عقوبات مباشرة على الأفراد والمؤسسات، إلا أن هذا يجعل الصين تمس حقوق التعبيرعن الرأي في الأنترنت، [92] فضلا عن المراقبة المكثفة للمحتويات الإلكترونية مما يُسهم في إكتشاف الأفعال غير المشروعة بسرعة، لذا فأنها تركز على السيطرة والسرعة في تلافي المحتويات المزيفة، وهذا خلاف ما انتهجه الإتحاد الأُوروبي في التصدي لجرائم التزييف العميق، وعن طريق قوانيها التي ذكرناها سابقًا، فانها تفرض على مقدمي الخدمات إعتماد مبدأ الشفافية بشأن المحتويات التي ينُشأونها والزامهم بالإبلاغ عن المحتوى المنُشئ بالذكاء الإصطناعي وتطبيق عقوبات مالية، والتي تفرض بشكل مبالغ قطعية أو تُحدد من نسب أرباح المؤسسات التي تتروح مابين 4% الى 6%، وتطبيق نظام إزالة المحتوى المزيف ومبدأ الشفافية. لذا إذا ما قارنا آليات التصدي بين الصين والإتحاد الأُوروبي، فأن الأخيرة تسمح بحرية التعبير عن الرأي على الأنترنت ويُعطي الأولية لحقوق الأفراد على خلاف موقف الصين، وهذه السياسية الجنائية تنعكس من النظام السياسي والإجتماعي لهما وفلسفتها في التصدي للجرائم ومكافحتها أو الوقاية منها. أما الولايات المتحدة الأمريكية، فنرى أنها مازالت تعتمد على قوانين عامة بالغالب في ظلّ غياب قانون فيدرالي شامل يعُد نهجًا لبقية الولايات، وعلى الرغم من وجود بعض القوانين الجزائية (التي اختلفت عقوباتها من ولاية لاخرى) أو مقترحات القوانين التي لم تُبصرْ النور إلى الآن، وربما هذا المشهد سيتغير بنهاية العام 2024 بعد اقرر مقترحات القوانين المذكورة آنفًا، فقد يتفق موقف قوانين الولايات المتحدة الأمريكية والإتحاد الأُوروبي من حيث الحفاظ على حرية التعبير، كم انها تتبع نهجًا متوازنًا لايتسمْ بالصرامة كما هو في الصين، كون الولايات المتحدة ملزمة دستوريًا بعدم تشريعها قوانين على المستوى الفيدرالي او الولايات يتناقض مع التعديل الأول من دستورها والذي يهدف إلى حماية التعبير، بما في ذلك الصور والفيديوهات، من تدخل الحكومة، مما يجعل القوانين التي تستهدف التزييف العميق تواجه تحديات دستورية، لذا نراها تعتمد مبدأ الموازنة بين الحريات والرقابة.

المطلب الرابع: الأُطر التقنية لمواجهة جرائم التزييف العميق.
Fourth Requirement: Technical Frameworks to Confront Deepfake Crimes.

لقد طورت الشركات العالمية والباحثون أدوات تقنية مختلفة تساهم في الكشف عن المحتويات المزيفة، ولعل أبرز هذه الأدوات:

التعلم العميق وتحليل البيانات، أن أدوات الكشف الحديثة تعتمد على شبكات عصبية عميقة منها (Convolutional Neural Networks (CNNs[93] و Recurrent Neural Networks (RNNs)، تعمل هذه الأداة على تحليل مكونات الصور- الفيديو، فضلًا عن إنها تُركز على إكتشاف الأنماط الدقيقة في الصور- الفيديو، منها حركة العين والملامح والتي قد تظهر غير متسقة في المحتوى المزيف.

العلامات المائية والتوقيع الرقمي (Digital Watermarking)، العلامة المائية نمط من البتات bits يتم إدخالها في صورة رقمية أو ملف صوتي أو فيديو لتحديد معلومات حقوق الطبع والنشر الخاصة بالملف (المؤلفون والحقوق وما إلى ذلك) وبالتالي فأن أي تزييف عميق يمكن إكتشافه [94]، لقد أعلنت شركة Adobe وTwitter وشركة The New York Times عن نظام جديد من أجل مكافحة إنتشار التلاعب بالمحتوى الرقمي وجرائم التزييف العميق عن طريق أصالة وشفافية المحتوى، وتعمل هذه المبادرة على تطوير أدوات تساهم في توثيق تاريخ ومصدر المحتوى الرقمي وسيسجل هذا النظام من أنشأ المحتوى وما إذا كان قد تم تعديله من قبل شخص آخر، ثم تسمح لأشخاص ومنصات أخرى بالتحقق من هذه البيانات. يطلق على هذا النظام أسم، "مبادرة أصالة المحتوى"the Content Authenticity Initiative(CAI)" ، من شأن علامة الإسناد أن تساعد في تتبع هذه الصور من لحظة الانتاج وضمان تتبعها عبر الانترنت عن طريق إدراج التوقيع الرقمي " حيث يتم تثبيت بيانات أدلة المحتوى بصورة مشفرة مع المحتوى لتكون قابلة للتحقق من اصالته من تأكد المتلقي لهذا المحتوى من مصدر المحتوى وتاريخ التعديلات عليه."[95].

التحليل الطيفي (Spectral Analysis)، تهدف تقنيات الكشف عن الصوت المزيف العميق إلى التمييز بين المقاطع الصوتية الأصلية والمولدة أو المعدلة بشكل مصطنع، أن هذه التقنية تعتمد على تحليل الترددات والإشارات في الصوت والفيديو، فضلا عن إنها تُستخدم للكشف عن الإختلافات الطفيفة التي لا يمكن للعين المجردة أو الأذن البشرية اكتشافها، منها التغييرات في تردد الصوت أو تباين الإضاءة في الفيديو[96].

التعاون بين الشركات والمؤسسات الاكاديمية، تتعاون شركات Google وشركة Meta (فيسبوك سابقًا) وتقدم للباحثين بيانات هائلة تحتوي على محتويات مزيفة

وحقيقية (صور – فيديوات) من أجل مساعدة الباحثين على تطوير تقنيات الكشف عن المحتويات المزيفة، فضلًا عن قيام شركة Meta بالتعاون مع شركة Amazonو شركة Microsoft وعددًا من المراكز البحثية والجامعات في أمريكا بالإعلان عن جوائز وحوافز ودعم مالي للباحثين من أجل تطوير وإيجاد تقنيات الكشف عن المحتوى المزيف. [97]

إن **الوعي العام ومحو الأمية الإعلامية" Public Awareness and Media Literacy"** من التدابير الأساسية لمكافحة هجمات الهندسة الإجتماعية والتلاعب المدعومة بالذكاء الإصطناعي. بدءًا من التعليم المبكر، يجب أن يكون الأفراد مجهزين بالمهارات اللازمة لتحديد المحتوى الحقيقي من المزيف، وفهم كيفية توزيع التزييف العميق، والتكتيكات الهندسية النفسية والإجتماعية التي تستخدمها الجهات الخبيثة. يجب أن تعطي برامج محو الأمية الإعلامية الأولوية للتفكير النقدي وتزويد الناس بالأدوات اللازمة للتحقق من المعلومات التي يستهلكونها. أظهرت الأبحاث أن محو الأمية الإعلامية مهارة قوية لديها القدرة على حماية المجتمع من التضليل المدعوم بالذكاء الإصطناعي، من خلال الحد من رغبة الشخص في مشاركة التزييف العميق. واخيرًا **عقلية عدم الثقة"Zero-Trust Mindset " في مجال الأمن السيبراني،** يعني نهج "عدم الثقة" عدم الثقة في أي شيء افتراضيًا والتحقق من كل شيء بدلاً من ذلك. وعند تطبيقه على البشر الذين يستهلكون المعلومات عبر الإنترنت، فإنه يتطلب جرعة صحية من الشك والتحقق المستمر. تتوافق هذه العقلية مع ممارسات اليقظة التي تشجع الأفراد على التوقف قبل الرد على المحتوى المحفز عاطفيًا والتفاعل مع المحتوى الرقمي عمدًا وبعناية. يساعد تعزيز ثقافة عدم الثقة من خلال برامج cybersecurity mindfulness programs (CMP) اليقظة للأمن السيبراني (CMP) في تجهيز المستخدمين للتعامل مع التزييف العميق والتهديدات السيبرانية الأخرى المدعومة بالذكاء الاصطناعي والتي يصعب الدفاع ضدها باستخدام التكنولوجيا وحده[98].

الخاتمة
Conclusion

بعد أن أنهينا دراستنا لــ ،" المواجهة الجنائية للجرائم الناشئة عن أستخدام تقنية التزييف العميق،" توصلنا إلى جملة من النتائج والتوصيات والتي سندرجها على النحو الآتي:-

أولًا: النتائجResult :-

1- لقد أدى التطور في علوم الكمبيوتر والذكاء الإصطناعي في ظهور تقنية التزييف العميق التي تعد أحد الظواهر المستحدثة التي تستخدم أذرع الذكاء الإصطناعي في تقديم خدمتها المشروعة أو غير المشروعة بعدها أدة أو وسيلة جرمية خطيرة وسهلة الوصول وقليلة الكلفة مما يجعلها أدة سهلة بيد المجرمين فتُصيب المصالح الجوهرية والمعتبرة التي يحرص المشرع أن يحميها كالسمعة والشرف والخصوصية ونزاهة الإنتخابات وغيرها.

2- أن التزييف العميق أحد تطبيقات الذكاء الإصطناعي والذي له القدرة على إنشاء محتويات رقمية (مرئية – صوتية) أو كليهما لشخص ما بصورة تُحاكي الواقع وتُخالف الحقيقية في نفس الوقت بقصد الإضرار به وتعريض المصالح المحمية قانونًا لضررًا أو خطرًا.

3- تتنوع الجرائم التي تُحدثها تقنية التزييف العميق، فبعض الجرائم تُصيب الأشخاص والمؤسسات الخاصة وجرائم التزييف العميق ضد الدولة والمؤسسات وتختلف انواع الجرائم التي تتحقق.

4- اختلفت الدول في معالجة الجرائم التي تنشأ بإستخدام تقنية التزييف العميق بقوانين مستقلة او تكييف النصوص العقابية التقليدية لمواجهة هذه الظاهرة، وعلى الرغم من تعدد هذه القوانين فهناك قصور تشريعي في معالجة جرائم التزييف العميق نظرًا للطبيعة المتطورة والسريعة لتقنية التزيف العميق الذي جعل من الصعب لهذه القوانين اللحاق بوتيره تطور هذه التقنية وبالتالي مكافحتها.

التوصياتRecommendations :-

1- يجب على السلطة التشريعية في دول العالم ولاسيما في العراق تبني إجراءات وسياسات واضحة في معالجة تقنية الذكاء الإصطناعي وتطبيقاتها مما يُسهم في وضع الإطار القانوني لتنظيمها وتلافي الانتهاكات التي تنجم عن استخداماتها غير المشروعة.

2- سن قانون خاص بالتزييف العميق يحدد معناه وأنواع الجرائم التي تنجم عن استخدامه وتحديد الجزاءات الجنائية والمدنية والإدارية. وبما أن المنظومة التشريعية في العراق تعاني من تأخر تشريعي في مجال تجريم الجرائم المعلوماتية أو السبيرانية ومازال القضاء يستعين بالنصوص التقليدية، لذا سنقترح مشروع قانون وطني خاص بالتزييف العميق، وعلى النحو الآتي:-

مشروع قانون مكافحة التزييف العميق وحماية الأمن الرقمي في جمهورية العراق

بأسم الشعب

رئاسة الجمهورية

بناءً على ما أقره مجلس النواب طبقًا لأحكام البند (أولًا) من المادة (61) والبند (ثانيًا) من المادة (72) من الدستور العراقي.

صدر القانون الآتي: رقم (.....) لسنة (.....)

المادة 1: التعاريف

أولًا: التزييف العميق: عملية تعديل أو تصنيع مقاطع الفيديو – الصوت – الصورة باستخدام خوارزميات الذكاء الاصطناعي، بقصد إنشاء محتوى مُزيف يُعرض للجمهور على نحو مضلل أو التأثير في الأفراد والمجتمع.

ثانيًا: المحتوى المُزيف: كُلّ محتوى يتم التلاعب فيه بهدف التأثير في الأفراد أو المجتمع، أو تحريف الحقائق بقصد التشهير، الإساءة، أو التأثير في الأمن العام والعمليات الديمقراطية في العراق.

المادة 2: الجرائم والعقوبات.

أولًا: يُعاقب بالحبس مدة لاتقل عن سنتين ولا تزيد عن خمس سنوات أو بغرامة لاتقل عن مليون دينار عراقي ولاتزيد عن خمسة مليون دينار عراقي، كل من يقوم بإنتاج أو نشر محتوى مزيف بهدف التضليل أو التشهير بالأشخاص أو من يحرز برامج أو أدوات بقصد ارتكابها في جرائم التزييف العميق، ويعاقب بنصف الحد الأقصى المقرر للعقوبة المقررة قانونًا في حالة الشروع.

ثانياً: تُشدد العقوبة إلى السجن الذي لايقل عن خمس ولايزيد عشر سنوات، والغرامة التي لاتقل خمسة مليون دينار عراقي ولاتزيد عشرة مليون دينار عراقي، ويعاقب بنصف الحد الأقصى المقرر للعقوبة المقررة قانونًا في حالة الشروع. إذا كان الهدف من المحتوى المزيف الإضرار بالأمن الوطني أو نشر الفتنه والكراهية أو التأثير في العمليات الانتخابية.

ثالثًا: يُعاقب بالسجن المؤبد كُلّ من يستخدم التزييف العميق من أجل إثارة العنف، أو التلاعب بالقرارات السيادية، ويعاقب بنصف الحد الأقصى المقرر للعقوبة المقررة قانونًا في حالة الشروع.

رابعًا: يُعاقب بالحبس مدة لا تقل عن سنتين ولا تزيد عن خمس سنوات والغرامة التي لاتزيد عن خمسة مليون دينار عراقي ومصادرة الادوات، كل من يُحرز أو يحتفظ بأي برامج أو أدوات تُستخدم في إنشاء أو تطبيقات التزييف العميق دون تصريح قانوني، أو دون وجود غرض مشروع. وتُشدد العقوبات لتصل إلى السجن لمدة لاتزيد عن عشر سنوات والغرامة التي لاتزيد عشرة مليون دينار عراقي، إذا تم استخدام البرامج المحتفظ بها في ارتكاب جريمة تؤدي إلى الابتزاز أو التشهير أو التلاعب بمعلومات أو بيانات تهدد الأمن القومي أو السلم الاجتماعي أو التزييف الذي يترتب عليه أضرار مادية أو معنوية جسيمة لشخص أو جهة. ويعفى من العقاب من يسلم الادوات للجهات المختصة قبل الاستخدام غير المشروع أو اثبت الحائز ان حيازته للادوات كانت لاغراض مشروعة.

المادة 3: استحداث آليات الكشف: بموجب هذا القانون يتم إنشاء هيئة مستقلة بأسم "*الهيئة الوطنية لأمن المعلومات*"، والتي تُعنى بالكشف عن المحتوى المزيف ورصد الجرائم السيبرانية، وتقديم الدعم الفني للجهات القانونية والمواطنين في كشف المحتوى المزيف ويجوز للهيئة التعاون مع الشركات الوطنية من أجل تطوير خوازميات تعتمد على الذكاء الإصطناعي من أجل المساهمة في كشف المحتوى المزيف.

المادة 4: التعاون مع الجهات الدولية: يجوز" للهيئة الوطنية لأمن المعلومات،" التعاون مع المنظمات الدولية والشركات العالمية المتخصصة من أجل تطوير التقنيات اللازمة لمواجهة التزييف العميق وتبادل الخبرات، وتعزيز الأمن الرقمي، وكذلك تفعيل تنفيذ أحكام القانون بشأن الجرائم العابرة للحدود التي تستهدف الدولة العراقية.

المادة 5: التوعية المجتمعية: تلتزم وزارة الإعلام بالتعاون مع وزارتي التعليم العالي والبحث العلمي ووزارة التربية بإطلاق حملات توعية مجتمعية لطلبة الكليات والمدارس واطلاق برامج لتدريب الصحفيين والمؤسسات الإعلامية حول مخاطر التزييف العميق وكيفية اكتشافه وتجنبه من أجل حماية الأفراد والمجتمع من التضليل الإعلامي والإنخراط في ارتكاب جرائم تنشأ باستخدام التزييف العميق.

المادة 6: حقوق التعبير والدفاع.

أولا:لا يُستخدم هذا القانون من أجل تضييق حرية التعبير أو الصحافة المحمية دستوريًا.

ثانيًا: يحق للمتهمين بنشر محتوى مزيف أستخدام كل طُرق الطعن المتاحة بموجب القوانين النافذه والتقاضي أمام محاكم مختصة يؤسسها مجلس القضاء الاعلى، على أن تشكل من قبل قاض أو أكثر من ذوي الخبرة والإختصاص.

المادة 6: تشديد عقوبات المنصات: يُلزم القانون كُلّ منصة رقمية أو وسيلة إعلامية باتخاذ إجراءات صارمة من أجل التحقق من المحتوى المنشور ومكافحة التزييف العميق وإلغاء المحتوى المزيف من على المنصة، وبخلافه تُفرض الغرامات المالية أو العقوبات الإدارية التي تصل لحد حجب المنصة في حالة تكرار المخالفات.

المادة 7: المسؤولية المجتمعية والتبليغ: تُشجّع الدولة المواطنين على الإبلاغ عن المحتوى المزيف والمشبوه عن طريق تحديد قنوات إتصال آمنة، مع توفير الحماية القانونية للمبلغين، وتثقيف الجمهور حول كيفية التحقق من المصادر الالكترونية وتجنب التضليل الإعلامي واتباع نهج "عدم الثقة".

المادة 8: أحكام ختامية: يدخل هذا القانون حيز النفاذ بعد تاريخ نشرهُ في الجريمة الرسمية.

الأسباب الموجبة:

يهدف هذا القانون الى توفير الحماية القانونية وإيجاد تنظيم قانوني لجرائم التزييف العميق والعمل على مكافحتها والوقاية منها ، وحماية المصالح المعتبرة قانونًا، التي يستهدفها التزيف العميق.

الهوامش
Endnotes

[1] Matthew B. Kugler and Carly Pace, *Deepfake Privacy: Attitudes and Regulation*, 116 Nw. U. L. Rev. 611 (2021). https://scholarlycommons.law.northwestern.edu/nulr/vol116/iss3/1 last seen in 11-11-2024.

[2]Oliver Lock , *Artificial Intelligence Guidance on Lexis+*,Produced in partnership with Oliver Lock of Farrer & Co,2024, https://www.lexisnexis.co.uk/legal/guidance/deepfakes last seen in 11-11-2024.

[3] اشرف سيد أبو العلا ، *المواجهة الجنائية لتقنية الديب فيك*، مجلة العلوم القانونية والاقتصادية،عدد66، الاصدار 3، 2024، الصفحات 477-511 ، صفحة 486، DOI: 10.21608/jelc.2024.342112.

[4] Pantserev, K.A., *The Malicious Use of AI-Based Deepfake Technology as the New Threat to Psychological Security and Political Stability*. In: Jahankhani, H., Kendzierskyj, S., Chelvachandran, N., Ibarra, J. (eds) Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity. Advanced Sciences and Technologies for Security Applications. Springer, Cham. (2020). (last seen in 3-11-2024) https://doi.org/10.1007/978-3-030-35746-7_3

[5] Mariëtte van Huijstee , Pieter van Boheemen ,Djurre Das and etal., *Tackling deepfakes in European policy*, *Panel for the Future of Science and Technology*, European Parliamentary Research Service, Scientific Foresight Unit (STOA), PE 690.039 – July 2021, p.2.

[6] Ki Chan, C. C., Kumar, V., Delaney, S., & Gochoo, M. (2020*). Combating Deepfakes: Multi-LSTM and Blockchain as Proof of Authenticity for Digital Media.* In 2020 IEEE / ITU International Conference on Artificial Intelligence for Good, AI4G 2020 (pp. 55-62). Article 9311067 (2020 IEEE / ITU International Conference on Artificial Intelligence for Good, AI4G 2020). Institute of Electrical and Electronics Engineers Inc.. https://doi.org/10.1109/AI4G50087.2020.9311067

[7] Claire Langlais-Fontaine: Démêler le vrai du faux: étude de la capacité dudroit actuel à lutter contre les deepfakes, La Revue des droits de l'homme, N°18 , 2020. P1. On website https://journals.openedition.org/revdh/9747 last seen 3-10-2024

[8] Europol, *Facing reality? Law enforcement and the challenge of deepfakes*, an observatory report from the Europol Innovation Lab, Publications Office of the European Union, Luxembourg.(2022). p6

[9] Bobby Chesney Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, California Law Review, Volume 107 , December (2019) p.1753. in the link https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security (last seen on 3-11-2024)

[10] Fatih ARSLAN, *Deepfake Technology*: A Criminological Literature Review,The Sakarya Journal of Law (The SJL), v. 11 section. 1 .p 701-720.p 704. file:///C:/Users/QAA/Downloads/DOC-20240827-WA0002..pdf

و عبدالله بن حسين الأسمري،تقنية التزييف العميق والذكاء الاصطناعي، وزارة الحرس الوطني - السعودية، 25-5-2023، اخر مشاهدة 3-10-2024،
https://kkmag.sang.gov.sa/Technicalarticles/Pages/%D8%AA%D9%82%D9%86%D9%8A%D8%A9-%D8%A7%D9%84%D8%AA%D8%B2%D9%8A%D9%8A%D9%81-%D8%A7%D9%84%D8%B9%D9%85%D9%8A%D9%82-%D9%88%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A1-%D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9%D9%8A.aspx

[11] Şeymanur Yönt, *The Deepfake Menace: Legal Challenges in the Age of AI*, TRT TRAINING AND RESEARCH DEPARTMENT ,March 2024,p6. Last seen in 5-10=2024 on file:///C:/Users/QAA/Downloads/The-Deepfake-Menace_v2.pdf and see also Durbin, R. J., & Graham, L., The DEFIANCE Act of 2024. https://www.durbin.senate.gov/imo/media/doc/defiance_act_of_2024.pdf

[12] Weatherbad, J. *Trolls have flooded X with graphic Taylor Swift AI fakes*. , January, 2024. The Verge. https://www.theverge.com/2024/1/25/24050334/x-twitter-taylor-swift-ai-fake-images-trending

[13]Vincent, J. Watch Jordan Peele use AI to make Barack Obama deliver a PSA about fake news. (2018, April 17). The Verge. https://www.theverge.com/tldr/2018/4/17/17247334/ai-fake-news-video-barack-obama-jordan-peele-buzzfeed

[14] Geller, E., & Vinocur, *N. French presidential candidate confirms 'massive' hack days before election.* (2017, May 5). Politico.

https://www.politico.com/story/2017/05/05/emmanuel-macron-french-election-hack-cyber-238059

[15] Ambrose, T. UK's enemies could use AI deepfakes to try to rig election, says James Cleverly. (2024, February 25). . The Guardian. https://www.theguardian.com/uk-news/2024/feb/25/uks-enemies-could-use-ai-deepfakes-to-try-to-rig-election-says-james-cleverly

[16] Şeymanur Yönt, *ad*, p6.

[17] Şeymanur Yönt, *ad*, p10.

[18] ينظر المادة 403 من قانون العقوبات العراقي رقم 111 لسنة 1969 المعدل.

[19]اشرف سيد أبو العلا، مصدر السابق، ص 381.

[20] قرر المشرع العراقي هذه القاعدة في المادة (141)من قانون العقوبات رقم 111 لسنة 1969، حيث نصت على أنه ،" إذا كون الفعل الواحد جرائم متعددة وجب إعتبار الجريمة التي عقوبتها أشد والحكم بالعقوبة المقرر لها، وإذا كانت العقوبات متماثلة حكم بإحداها." وينظر كذلك المادة 25 من قانون مكافحة جرائم تقنية المعلومات المصري رقم 175 لسنة 2018 على الرابط https://manshurat.org/node/31487

[21] عرفت المادة 19 فقرة 3/ د، من قانون العقوبات العراقي رقم 111 لسنة 1969 المعدل العلانية بقولها ،" الكتابة والرسوم والصور والاشارات والافلام ونحوها اذا عرضت في مكان مما ذكر او إذا وزعت او بيعت إلى أكثر من شخص او عرضت للبيع في أي مكان." كما قررت محكمة استئناف بغداد الرصافة الاتحادية بصفتها التمييزية بالرقم 989 / جزاء / 2014 والذي اعتبرت فيه موقع التواصل الاجتماعي الفيس بوك من وسائل العلانية.

[22] ذكر تقرير يوروبول حول تقنية التزييف العميق في عام 2022 (Criminal Use of Europol Report Deepfake Technology) والذي اوضح ،"أن تقنية التزييف العميق باتت تستخدم على نطاق واسع عبر منصات الإنترنت لأهداف إجرامية تشمل الاحتيال المالي، تزوير الوثائق، نشر الأخبار الكاذبة، والتأثير على الرأي العام، إضافة إلى استخدامها في الجرائم الجنسية مثل نشر محتوى جنسي غير توافقي. لذا، فإن هذه التقنية تتطلب وجود تشريعات حديثة وأساليب متطورة للحد من آثارها الضارة، فضلا عن الحاجة إلى سياسات دولية صارمة لضبط استخدام أدوات التزييف العميق وفرض المسؤولية على جميع الأطراف المعنية في تطويرها ونشرها." متوفر على الرابط ادناه اخر زيارة 29-10-2024.

/https://eucrim.eu/news/europol-report-criminal-use-of-deepfake-technology

[23] د. محمود سلامة عبدالمنعم،جريمة الانتقام الإباحي عبر تقنية التزييف العميق " Deepfakes " والمسؤولية الجنائية عنها،المجلد 2.2022، العدد 1، يوليو 2022، الصفحة 485-366 . ص 384. على الرابط الالكتروني، https://lalexu.journals.ekb.eg/article_266089.html اخر مشاهدة 27-10-2024.

24 أن الاسناد ينقسم الى الاسناد المادي والاسناد المعنوي فالإسناد المادي يتطلب توافر رابط مادي "الرابطة السببية" التي تربط بين الفعل الإجرامي للإنسان والنتيجة الجرمية لإيمكن إسنادها للجاني من الناحية المادية، ويتطلب كذلك وجود صلة معنوية بين الأثنين كذلك الإرادة الواعية الحرة كمتطلب لإنعقاد المسؤولية الجزائية للجاني. للمزيد ينظر، أحمد لطفي السيد مرعي، إنعكاسات تقنيات الذكاء الإصطناعي على نظرية المسؤولية الجنائية: دراسة تأصيلية مقارنة، مجلة البحوث القانونية والإقتصادية، جامعة المنصورة-كلية الحقوق، عدد2022،80،الصفحات 399-244، ص312.

[25] Europol , Facing reality? Law enforcement and the challenge of deepfakes, an observatory report from the Europol Innovation Lab, Publications Office of the European Union, Luxembourg.(2022). P9-10. مذكور تاليا

[26] Criminal Use of Deepfake Technology Europol Report of 2022on website last seen 29-10-2024. https://eucrim.eu/news/europol-report-criminal-use-of-deepfake-technology/

[27]محمود سلامة عبدالمنعم،مصدر سابق، ص 386.

[28] تتنوع الجرائم التي تحدثها تقنية التزييف العميق، فبعض الجرائم تصيب الاشخاص والمؤسسات الخاصة) ومن هذه الجرائم (جرائم الابتزاز والانتقام الاباحي العميق-جرائم الاحتيال العميق-جرائم تشويه السمعة والانتقام- جرائم التزييف العميق في التجسس وسرقة المعلومات الحساسة) وجرائم التزييف العميق ضد الدولة والمؤسسات العامة ومن هذه الجرائم (جرائم التزييف العميق ضد الدولة ورجال الانتخابات-جرائم التزييف العميق ضد الصحافة والاعلام- جرائم التزييف العميق ضد نظام العدالة والقضاء- جرائم التزييف العميق ضد آمن واستقرار الدولة) للمزيد ينظر علاء الدين منصور مغايرة، جرائم الذكاء الاصطناعي وسبل مواجهتها، جرائم التزييف العميق نموذجًا، المجلة الدولية للقانون، جامعة قطر، المجلد 13، العدد المنتظم الثاني، 2024، https://doi.org/10.29117/irl.2024.0301 اخر مشاهد 3-11-2024.

[29] ان تقنية التزييف العميق تؤثر في حقوق الإنسان أثناء الانتخابات. تنص المادة 25 من العهد الدولي الخاص بالحقوق المدنية والسياسية على حق كل فرد في المشاركة في إدارة الشؤون العامة والتصويت. وقد استُخدم التزييف او الاخبار الكاذبة (التزييف العميق) على نطاق واسع أثناء الانتخابات أو الاستفتاءات للتلاعب بالناخبين وتشكيل نتائج استطلاعات الرأي. كما استُخدمت الروبوتات للتأثير في المناقشة العامة والتأثير على الناخبين في الانتخابات المحلية والدولية. في الإكوادور والفلبين، اعترف الرئيسان باستخدام متصيدين مدفوعي الأجر أثناء الحملات الانتخابية. وأكدت الدراسات أيضًا استخدام الدعاية التي تقودها الدولة من قبل وكالة أبحاث الإنترنت الروسية كتكتيك للسياسة الخارجية للتأثير على نتائج الانتخابات الرئاسية الأمريكية لعام 2016. تم تقديم معلومات مضللة وخادعة لمجموعات مستهدفة لتقويض حقها في التصويت. كما تم استخدام حملات مماثلة لتشويه سمعة بعثات مراقبة الانتخابات ينظر في ذلك

RESEARCH PROJECT ,*Misinformation and Misinformation and Deepfakes*,on the website of university of Essex/Human Rights Big Data and Technology Law Enforcement. (without name and date) last seen in 11-11-2024 . https://www.essex.ac.uk/research-projects/human-rights-big-data-and-technology/misinformation-and-disinformation-and-deep-fakes

[30]التهديدات التي يتعرض لها المدافعون عن حقوق الإنسان والصحفيون والتأثير المخيف بتقنية التزييف العميق، إذ يمكن أيضًا استخدام "الدعاية الحاسوبية" لاستهداف أو مضايقة الصحفيين والمدافعين عن حقوق الإنسان المنتقدين للحكومات أو الحركات السياسية. وقد يشمل ذلك الرعاية الرسمية من جانب الدولة وغيرها من الجهات الراعية من جانب المنظمات. والهدف من هذا الاستهداف هو إحداث ضرر بالسمعة، أو رد فعل عنيف من جانب المجتمع، أو إحداث تأثير مخيف يثبط عزيمة الاستمرار في العمل النقدي، كما حذر الأمين العام للأمم المتحدة في كلمته الافتتاحية أمام مجلس حقوق الإنسان في فبراير/شباط 2019. ويمكن أن تخلف حملات التحرش عبر الإنترنت تأثيراً مخيفاً على حرية التعبير وتكوين الجمعيات والتجمع للأفراد المستهدفين، الذين قد يمتنعون عن التعبير علناً عن آرائهم والانخراط في أنشطتهم العادية خوفاً من المزيد من الاعتداءات اللفظية والجسدية. المصدر السابق. على الرابط https://www.essex.ac.uk/research-projects/human-rights-big-data-and-technology/misinformation-and-disinformation-and-deep-fakes

[31]لقد عملت الدول والشركات والمنظمات الدولية على تطوير استجابات لمعالجة التضليل/المعلومات المضللة، بدءًا من إنشاء مجموعات الخبراء وفرق العمل، وخفض رتبة/إزالة المحتوى والحسابات، وقوانين مكافحة التضليل وبرامج محو الأمية الإعلامية. وقد تشكل بعض هذه التدابير مخاطر إضافية على حقوق الإنسان، وخاصة حرية التعبير. المصدر السابق.
https://www.essex.ac.uk/research-projects/human-rights-big-data-and-technology/misinformation-and-disinformation-and-deep-fakes

[32] Meskys, Edvinas and Kalpokiene, Julija and Jurcys, Paul and Liaudanskas, Aidas, *Regulating Deep Fakes*: Legal and Ethical Considerations (December 2, 2019). Journal of Intellectual Property Law & Practice, Volume 15, Issue 1, January 2020, Pages 24–31., Available at SSRN: https://ssrn.com/abstract=3497144 _
أن جريمة الانتقام الاباحي بصورة عامة تعني نشر صور ومقاطع جنسية لشخص ما كوسيلة لعقابه أو إيذائه، ويحدث هذا السلوك كرد فعل عند انفصال شريكين أو حبيبين سابقين ، كما قد يكون الهدف من النشر الحصول على مكاسب مادية أو لارضاء شعور غريزي أو اشباع جنسي لدى الفاعل أو نشرها في موقع اباحي حاص به

[33] Edvinas Meskys, and etal, *ida*, p.7.

[34]د. محمود سلامة عبدالمنعم، مصدر سابق، ص392 .

[35] Edvinas Meskys, and etal , *ida*,.p. 5 .

[36] P Hayward, A Rahn, '*Opening Pandora's Box: pleasure, consent and consequence in the production and circulation of celebrity sex videos'* (2015) 2(1) Porn Studies 49 .https://doi.org/10.1080/23268743.2014.984951

[37] EM Ellis, '*People Can Put Your Face on Porn—and the Law Can't Help You'*, (available at: https://www.wired.com/story/face-swap-porn-legal-limbo) .

[38] S. Bates, '"*Stripped": An Analysis of Revenge Porn Victims' Lives after Victimization'*, Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Arts/ SIMON FRASER UNIVERSITY. 2012. P. 18, (available at: https://summit.sfu.ca/item/15668)

[39] Edvinas Meskys, and etal, *ida*, p.8.

[40] كانت نائبة الرئيس الأمريكي كامالا هاريس ضحية لإعادة إنتاج، حيث تم استبدال الصوت الأصلي لخطابها بمادة مهينة. كان صوتها متقطعًا، مما أعطى انطباعًا خاطئًا بأنها ربما كانت في حالة سُكر ، كما صور الفيديو المزيف الممثل الشهير مورغان فريمان، الذي يُزعم أنه انتقد الرئيس الامركي جو بايدن، واصفًا إياه بأنه "أحمق". وقد شاهد الآلاف من مستخدمي X اللقطات المزيفة . المصدر السابق.

[41] Edvinas Meskys, and etal, *Ida*, p.7.

[42] في انتخابات الرئاسة في امريكام لعام 2016 ، لعبت المعلومات المضللة التي نشرت على شكل مقاطع فيديو مزيفة على فيسبوك ومنصة x تويتر سابقًا، تظهر المرشحين للانتخابات يقولون أو يفعلون مالم يقولوه او يفعلوه بالواقع . على سبيل المثال، لقد تم الترويج عن مقاطع فيديو مزيفية تظهر الرئيس الامريكي الحالي جو بايدن بمقاطع فديو مزيفة باستخدام تقنية التزييف العميق تظهره (يتحدث ببطء شديد- يدلي بتصريحات سياسية حول قضايا معينة مثل الهجرة والاقتصاد – عدم احترامه لطوائف معينة في المجتمع) من اجل احداث تأثير سلبي في الناخبين وتشويه سمعته السياسية، لذا تقوم بعض منصات التواصل الاجتماعي كمنصة أكس وفيسبوك تطيرها ادوات تعزز من قدرتها على رصد المحتويات الزائفة وتميزها عن المحتويات الحقيقية فضلا عن تنبيه المستخدمين . للمزيد ينظر

Emily Hallas, How battleground states are targeting AI and 'deepfakes' in political campaigns, 7-10-2024 on the link below https://www.washingtonexaminer.com/news/campaigns/3176252/battleground-states-targeting-ai-deepfakes-campaigns/ last seen 28-10-2024.

[43] Lewrence Norden,Niyti Narang,Laura J. , *States Take the Lead in Regulation AI in Elections Within Limits*, Brennan Center For Justices, published in Augest 7,2024. Last seen 29-2024 on the link below https://www.brennancenter.org/our-work/research-reports/states-take-lead-regulating-ai-elections-within-limits

[44] S> 2691 -AI Labeling Act of 2023. https://www.congress.gov/bill/118th-congress/senate-bill/2691/text

Sec.2/ a. Disclosures for AI generated content says," (a) Consumer disclosures.— (1) IMAGE, VIDEO, AUDIO, OR MULTIMEDIA AI-GENERATED CONTENT.— (A) IN GENERAL.—Each generative artificial intelligence system that, using any means or facility of interstate or foreign commerce, produces image, video, audio, or multimedia AI-

generated content shall include on such AI-generated content a clear and conspicuous disclosure that meets the requirements of subparagraph (B). (B) DISCLOSURE REQUIREMENTS.—A disclosure required under subparagraph (A) shall meet each of the following criteria:(i) The disclosure shall include a clear and conspicuous notice, as appropriate for the medium of the content, that identifies the content as AI-generated content.
(ii) The output's metadata information shall include an identification of the content as being AI-generated content, the identity of the tool used to create the content, and the date and time the content was created.
(iii) The disclosure shall, to the extent technically feasible, be permanent or unable to be easily removed by subsequent users

[45] Lewrence Norden,Niyti Narang,Laura J, *ida.*

[46] علاء الدين منصور مغايره، مصدر سابق، ص 147.

[47]تعمل الحكومة الكورية الجنوبية كدولة في قارة أسيا، على تنظيم استخدام التزييف العميق لإنشاء محتوى جنسي ضار. في نهاية سبتمبرمن عام 2023، أقرت لجنة الجمعية الوطنية مشروع قانون من شأنه أن يفرض عقوبة الحبس التي تصل إلى ثلاث سنوات أو غرامة قدرها 30 مليون وون على الأشخاص الذين ينشئون أو يستهلكون محتوى جنسيًا مزيفًا عميقًا. كما أقروا مشروع قانون يشدد العقوبات على استخدام المواد الجنسية لإكراه القاصرين. وقبل هذه الإجراءات التشريعية، أكد المشرعون على الدعم الحزبي لمعالجة الأضرار الناجمة عن المحتوى المزيف العميق.

Terrence Matsuo, *Deepfakes and Korean Society:* Navigating Risks and Dilemmas,October 3, 2024

On the link last see 1-11-2024 , https://keia.org/the-peninsula/deepfakes-and-korean-society-navigating-risks-and-dilemmas/

اما في الهند، لا توجد قوانين محددة في الهند لمعالجة الجرائم المتعلقة بالتزييف العميق والذكاء الإصطناعي، ولكن الأحكام الواردة في عدد كبير من التشريعات التي يمكن أن تقدم معالجات مدنية وجنائية. على سبيل المثال، ينطبق القسم 66 من the Information Technology Act, 2000 (IT) قانون تكنولوجيا المعلومات لعام 2000 (قانون تكنولوجيا المعلومات) في حالات جرائم التزييف العميق التي تنطوي على التقاط أو نشر أو نقل صور شخص ما في وسائل الإعلام الجماهيرية وبالتالي انتهاك خصوصيته. يعاقب على مثل هذه الجريمة بالحبس لمدة تصل إلى ثلاث سنوات أو غرامة قدرها 200 ألف روبية. وبالمثل، يعاقب القسم 66 Dمن قانون تكنولوجيا المعلومات الأفراد الذين يستخدمون أجهزة الاتصال أو موارد الكمبيوتر بنية خبيثة، مما يؤدي إلى انتحال الشخصية أو الغش. تصل عقوبة الجريمة بموجب هذا الحكم إلى الحبس لمدة تصل إلى ثلاث سنوات و/أو غرامة قدرها 100 ألف روبية.علاوة على ذلك، يمكن استخدام الأقسام 67 و67 A و67B من قانون تكنولوجيا المعلومات لمقاضاة الأفراد لنشرهم أو نقل التزييف العميق الفاحش أو الذي يحتوي على أي أفعال جنسية صريحة. كما تحظر قواعد تكنولوجيا المعلومات استضافة "أي محتوى ينتحل شخصية شخص آخر" وتتطلب من منصات وسائل التواصل الاجتماعي إزالة "صور

مشوهة بشكل مصطنع" للأفراد بسرعة عند تنبيههم. وفي حالة فشلهم في إزالة مثل هذا المحتوى، فإنهم يخاطرون بفقدان حماية "الملاذ الآمن" - وهو حكم يحمي شركات وسائل التواصل الاجتماعي من المسؤولية التنظيمية عن المحتوى التابع لجهات خارجية والذي يشاركه المستخدمون على منصاتهم. يمكن أيضًا اللجوء إلى أحكام قانون العقوبات الهندي لعام 1860 (IPC) للجرائم الإلكترونية المرتبطة بالتزييف العميق - المواد 509 (الكلمات أو الإيماءات أو الأفعال التي تهدف إلى إهانة حياء المرأة)، و499 (التشهير الجنائي)، و153 (أ) و(ب) (نشر الكراهية على أسس طائفية) من بين أمور أخرى. وبحسب ما ورد سجلت وحدة شرطة دلهي الخاصة بلاغًا ضد أشخاص مجهولين من خلال الاستعانة بالمادتين 465 (التزوير) و469 (التزوير للإضرار بسمعة أحد الأطراف) في قضية ماندانا.للمزيد في موقف الهند من الجريمة

Vig, Shinu. "*Regulating Deepfakes: An Indian perspective*." Journal of Strategic Security 17, no. 3 (2024) : 70-93.
DOI: https://doi.org/10.5038/1944-0472.17.3.2245 Available at: https://digitalcommons.usf.edu/jss/vol17/iss3/5

[48]China Law Translate ,Provisions on the Administration of Deep Synthesis Internet Information Services ,on the link https://www.chinalawtranslate.com/en/deep-synthesis/ دخل القانون حيز النفاذ في 10 يناير 2023.

[49] Article 7 of the Administration of Deep Synthesis Internet Information Services.

[50] Article 9 of the Administration of Deep Synthesis Internet Information Services.

[51] Article 10 of the Administration of Deep Synthesis Internet Information Services.

[52] ان العلامة المائية تعد علامة مرئية أو غير مرئية تتم اضافتها لصورة أو فيديو للاشارة الى مالكها أو مصداقيتها، فضلا عن، انها تستخدم عادة لمنع التلاعب بالمحتويات الالكترونية ، وهذه العلامة تتخذ شكل (نصًا – رمزًا- نمطًا) معينًا داخل المحتوى الرقمي . كما ان الخبراء طورا علامة مائية ذكية خاصة بالتزييف العميق إذ يمكن التعرف على الفيديو المزييف ليبدو اقل وضوحا من المحتوى الاصلي. علاء الدين منصور مغايرة، مصدر سابق، ص 149.

[53] Article 16 of the Administration of Deep Synthesis Internet Information Services.

[54] علاء الدين منصور مغايرة، مصدر سابق، ص 149.

[55] بالنسبة للتشريع العراقي، لايوجد قانون يعالج الجرائم الناشئة عن تقنية deepfake بصورة صريحة ، وعليه يتم اللجوء لعدة قوانين لسد هذه الفجوة التشريعية، ومنها، قانون العقوبات العراقي رقم 111لسنة 1969 المعدل ،على الرغم من عدم وجود نصوص صريحة في القانون لوضعه بزمان سبق نشأة هذه التقنية، إلا أنه يُمكن الاستعانة بنص المادة 286 (في حالات التزوير في المحررات – الصور بتقنية التزييف العميق) ، المواد (433و434 حالات التشهير بالاشخاص بتقنية التزييف

العميق) ، المادة 456 (جرئم الاحتيال بواسطة هذه التقنية)، المواد التي عالجت الابتزاز والتهديد المادة 430(التهديد بارتكاب جناية) والمادة (431) التهديد الشفوي أو الكتابي بجريمة غير الجنايات (...إذا كان التهديد في خطاب خال من أسم مرسله أو كان منسوبًا صدوره لجماعة سرية....) ، والمواد التي عالجت التحريض على الكراهية (المواد 200 و210و403) كما يمكن الاستعانة بنصوص قانون مكافحة الارهاب رقم (13) لسنة 2005، لم يتضمن هذا القانون بصورة صريحة جرائم التزييف العميق إلا انه يمكن تطويع النص العقابي اذا ماتم استخدام التزييف العميق أداة لتحقيق الاهداف الارهابية منها تهديد الأمن القومي او التحريض على العنف واثارة الذعر وغيرها (المواد 2-4-5) كما يجب أن يتم إثبات أن استخدام التزييف كان وسيلة لتحقيق العمل الارهابي وهذه مسألة يقررها القاضي حسب ظروف كل قضية، كما يمكن استخدام قانون هيئة الاعلام والاتصالات رقم 65 لسنة 2004 (التي تأسست بموجب الأمر 56 في 2004) وبموجب لوائح الهيئة فأنها تمنع نشر المحتويات التي تساهم في تضليل الجمهور او التحريض على العنف والكراهية ومحاسبة وسائل الاعلام ومن ضمنه اذا تم استخدام التزييف العميق وكذلك قانون حقوق المؤلف رقم (3) لسنة 1971 المعدل المادة (8) التي اشارت لحقوق المؤلف الادبية- المالية على اعماله الأصلية وعليه يمنع على أي شخص تعديل –تحريف- نشر وتزييف هذا العمل دون أخذ الموافقة الكتابية من المؤلف نفسه أو ورثته بعد موته، فإذا استخدم التزييف العميق على هذه المصنفات فبالامكان إعمال هذه المادة ، والمادة (47) التي حددت الجزاءات الجنائية التي تمثلت بالحبس والغرامة لمن ينتهك الحقوق المنصوص عليها قانونًا للمؤلف بموجب هذا القانون ومن ضمن صور الانتهاك التزييف العميق. الى الان قانون الجرائم المعلوماتية لم يُسّن ولايتضمن نصوص تتعلق بالتزيف العميق أو تعريفها، لذا الحاجة تدعو لوجود قانون يتعامل بصورة مباشرة مع هذه التقنية أو ادخال مواد قانونية لقانون العقوبات العراقي من اجل ضمان معالجة هذه الجرائم، وضمان عدم افلات الجناة من قبضة العدالة بسبب هذا القصور التشريعي.

[56] Identity Theft and Assumption Deterrence Act. As amended by Public Law 105-318, 112 Stat. 3007 (Oct. 30, 1998) on website https://www.ftc.gov/legal-library/browse/rules/identity-theft-assumption-deterrence-act-text

[57] [57] Mohamed Chawki, Navigating legal challenges of deepfakes in the American context: a call to action, Cogent Engineering, (2024) .p9. 11:1, 2320971, DOI: 10.1080/23311916.2024.2320971

[58]Identity Theft and Assumption Deterrence Act 18 U.S.C. § 875(c) charges or imprisons a person for two years if the person: 1. Knowingly makes a communication containing a true threat to injury in interstate commerce or foreign commerce, and 2. Intends the communication to be a true threat to injure another or knows that the recipient of the threat would understand it to be a threat

[59] 9-48.000 - Computer Fraud and Abuse Act, on website https://www.justice.gov/jm/jm-9-48000-computer-fraud

[60] Mohamed Chawki, *Ida* at p.7.

[61] Federal cyberstalking statutes. 18 U.S.C. § 2261 A applies to conduct that" 'places [a] person in reasonable fear of the death of, or serious bodily injury to […] (i) That person; (ii) an immediate family member; or (iii) a spouse or intimate partner of that person'. The defendant must have the mens rea to 'kill, injure, harass, intimidate or place [the victim] under surveillance".

[62] Identifying Outputs of Generative Adversarial Networks Act https://www.govtrack.us/congress/bills/116/s2904

[63] كما تم طرح مشروع قانون المسمى S.3805 - Malicious Deep Fake Prohibition Act of 2018 والذي تمت قرأته مرتين من قبل مجلس الشيوخ - 2018/12/21 قُرئ مرتين وأُحيل إلى لجنة القضاء. يعدل هذا القانون المادة 18 من قانون الولايات المتحدة لحظر إنشاء وتوزيع "التزييف العميق" - وهي تسجيلات صوتية بصرية تبدو زوراً وكأنها تسجيلات أصلية لخطاب أو سلوك فرد ما. ويجعل مشروع القانون إنشاء أو توزيع التزييف العميق بقصد تسهيل السلوك الإجرامي أو الضار بموجب القانون الفيدرالي أو الولائي أو المحلي أمرًا غير قانوني. ويمكن تغريم المخالفين و/أو سجنهم، مع فرض عقوبات أشد على التزييف العميق الذي قد يؤثر في إجراءات الحكومة أو يسهل العنف. ويتضمن مشروع القانون أيضًا حماية لمقدمي خدمات الكمبيوتر التفاعلية الذين يتخذون إجراءات لتقييد الوصول إلى التزييف العميق أو توفير الوسائل التقنية لتقييد الوصول إليه، فضلاً عن الحماية للأنشطة المحمية بموجب التعديل الأول. ينشئ هذا القانون جريمة جنائية جديدة تتعلق بإنشاء أو توزيع سجلات إعلامية إلكترونية مزيفة تبدو واقعية. للمزيد ينظر مسودة المشروع على الموقع الكونغرس الامريكي. اخر زيارة 11-11-2024 على الرابط الكونغرس الامريكي
https://www.congress.gov/bill/115th-congress/senate-bill/3805/text

[64] DEEP FAKES Accountability Act of 2020 on the link after, https://www.congress.gov/bill/116th-congress/house-bill/3230#:~:text=It%20establishes%20new%20criminal%20offenses,years%20in%20prison%2C%20or%20both.

[65] Article 1041 Sec 2B Accountability FAKES DEEP Act 2020.

[66] Article 1041 Sec 2C (1) Accountability FAKES DEEP Act 2020.

[67] Article 1041 Sec 2C (1) Accountability FAKES DEEP Act 2020

[68] Article 1041 Sec 2F (1) Accountability FAKES DEEP Act 2020

[69] Article 1041 Sec 2F (2) Accountability FAKES DEEP Act 2020

[70] Article 1042 Sec 2 Accountability FAKES DEEP Act 2020

[71] Article 1042 Sec 3 (1)2(Accountability FAKES DEEP Act 2020

[72] Article 918 Sec (7) (A) A Accountability FAKES DEEP Act 2020

[73]كمسألة أولية، فإن قانون حقوق الطبع والنشرCopyright Law هو وسيلة لن تنجح على الأرجح في الحد من عمليات التزييف العميق الخبيثة. وذلك لأن عمليات التزييف العميق في معظمها تُصنع لأغراض غير تجارية، ومن المرجح أن تكون نتائج عملية التزييف العميق "تحويلية"'transformative'.. في قضية و,Dhillon v. Doe، ادعت محكمة المقاطعة للمنطقة الشمالية من كاليفورنيا، الولايات المتحدة الأمريكية، أن استخدام صورة شخصية سياسية في موقع ويب غير تجاري لإدانة الشخصية السياسية كان "متصورًا تمامًا باعتباره استخدامًا عادلاً نموذجيًا بموجب قانون حقوق الطبع والنشر" وقد صدق هذا التحليل على عمليات التزييف العميق أيضًا. على سبيل المثال، حاول الفنان الموسيقي جاي زي استخدام ضربة حقوق الطبع والنشر لإزالة صوته المزيف العميق من يوتيوب. ومع ذلك، لم ينجح الإضراب، ولا يزال من الممكن العثور على مقطع فيديو لجاي زي وهو يتلو مونولوج "أن نكون أو لا نكون" من مسرحية هاملت و"لم نشعل النار" لبيلي جويل على الإنترنت. إن المبدأ الأساسي لقانون حقوق الطبع والنشر هو أن التعبيرات المعينة فقط وليس الأفكار أو الحقائق مؤهلة للحصول على حقوق الطبع والنشر. وهذا يستلزم سؤالاً أعمق فيما يتعلق بالتزييف العميق: هل وجه الشخص أو صوته خاضع لحقوق الطبع والنشر؟ والإجابة هي أن الصوت أو الوجه غير قابل للحماية بموجب قانون حقوق الطبع والنشر .وقد قضت المحكمة في قضية Butler v. Target بأنه على الرغم من أن كلمات الأغنية خاضعة لحقوق الطبع والنشر، فإن

الصوت الأساسي ليس كذلك، حيث لا يوجد حد لعدد الكلمات أو العبارات التي يمكن للشخص أن ينطق بها بصوته المميز. بالإضافة إلى ذلك، من المحتمل أن تندرج التزييف العميق ضمن الأعمال المشتقة بموجب 17 U.S.C. §103 وبالتالي، فإن أي حماية لحقوق الطبع والنشر موجودة لن يتم توسيعها لتشمل التزييف العميق. إن حماية حقوق الطبع والنشر ببساطة لا تمتد إلى الصفات المتأصلة للشخص . للمزيد ينظر الموقع في قضية Dhillon v. Doe,، https://casetext.com/case/dhillon-v-doe-1 وقضية Butler v. Target https://casetext.com/case/butler-v-target-corporation .

[74]بموجب المادة 230 من قانون آداب الاتصالاتUnder § 230 of the Communications Decency Act ، لا تتحمل مواقع الويب المسؤولية عن المحتوى المنشور من قبل أطراف ثالثة. إذا أنشأ شخص ما مقطع فيديو مزيفًا ونشره على موقع تابع لجهة خارجية، فإن هذا الموقع التابع لجهة خارجية لا يتحمل المسؤولية القانونية عن الفيديو. فسرت المحاكم قانون آداب الاتصالات على نطاق واسع على أنه يعزل هذه الأطراف الثالثة عن جميع المسؤولية المدنية، باستثناء المسؤولية عن انتهاك حقوق الطبع والنشر. على سبيل المثال، في قضية بارنز ضد شركة ياهوBarnes v. Yahoo, Inc. ، ، قررت الدائرة التاسعة أن المادة 230 تحظر المطالبة بـ "عدم تقديم الخدمات" عندما لم تقم ياهو بإزالة الصور الجنسية الواضحة للمدعية التي عرضها صديقها السابق. إن هذا التعويض يشكل مشكلة كبيرة للأفراد مثل السيدة مارتن، حيث أنه من الصعب أو حتى من المستحيل العثور على المبدعين الفعليين للفيديوهات المزيفة. ومع ذلك، بافتراض أنه يمكن استنتاج الأرباح من عائدات الإعلانات الشخصية المكتسبة من عرض الفيديو المزيف، فإن أي مطالبة ستظل بحاجة إلى صياغتها وفقًا لقانون الولاية. لا تعترف حوالي عشرين ولاية بحق الدعاية، ومن بين تلك الولايات التي تعترف بذلك، لا يوجد لدى معظمها لغة موجهة صراحةً نحو تكنولوجيا

الفيديو المزيف. أصبحت نيويورك مؤخرًا أول ولاية توسع صراحةً حق الفرد في الدعاية لتشمل الصور المولدة بواسطة الكمبيوتر أو النسخ الرقمية. بالإضافة إلى ذلك، يمتد الحق في الدعاية لمدة أربعين عامًا بعد وفاة الفرد. ومع ذلك، لا ينبغي للمتقاضين أن يتوقعوا من معظم الولايات أن توسع صراحةً حق الدعاية لتشمل الصور المولدة بواسطة الكمبيوتر في أي وقت قريب. ومع ذلك، هناك دائمًا مطالبات بالتشهير متاحة للأشخاص الذين هم موضوع تزييف عميق خبيث . للمزيد تنظر القضية على الرابط https://casetext.com/case/barnes-v-yahoo-inc-3

[75]اعتمادًا على ما إذا كان موضوع اللغة التشهيرية المزعومة شخصية عامة/مسؤولًا أو فردًا عاديًا، فإن المعايير القانونية للدعوى تتغير عادةً ما يتم تقسيم جريمة التشهير إلى شكلين من أشكال الكلام التي لا يحميها التعديل الأول: التشهير (الاتصالات المكتوبة أو المماثلة مثل التزييف العميق) والقذف (الاتصالات المنطوقة). في حين تختلف قوانين التشهير من ولاية إلى أخرى، فإن إعادة صياغة الجرائم الثانية توفر العناصر التالية لإثبات المسؤولية عن التشهير: (أ) خطاب كاذب ومسيء بشأن شخص آخر؛ (ب) نشر غير مخصص لطرف ثالث؛ (ج) إهمال من جانب الناشر يسبب ضررًا؛ و(د) إما أن يكون الخطاب قابلاً للمساءلة دون الحاجة إلى ضرر خاص أو وجود ضرر خاص ناجم عن النشر. ومع ذلك، فإن العنصر الثالث من التشهير، (ج)،يختلف بالنسبة للمسؤولين العموميين أو الأشخاص الذين هم في ضوء عام. في قضية New York Times Co. v. Sullivan، قضت المحكمة العليا بأنه عندما يكون الخطاب المعني موجهًا إلى شخصية سياسية أو ينتقد السلوك الرسمي، يتم استبدال معيار "الإهمال"negligence‘ ’ بمعيار أعلى لإثبات أن المتحدث تصرف بحقد فعلي. وقد عرّفت المحكمة "الحقد الفعلي" ‘actual malice’ بأنه الخطاب الذي تم الإدلاء به "مع العلم أنه زائف أو بتجاهل متهور للحقيقة". يتطلب إنشاء تزييف عميق مقنع حاليًا مستوى معينًا من إتقان الكمبيوتر. وعلاوة على ذلك، يجب جمع صور وجه متعددة للموضوع، ويجب اختيار مقطع الفيديو المضيف بعناية لضمان المظهر الحقيقي. لذلك، مع التكنولوجيا الحالية، قد يكون من المستحيل تقريبًا إنشاء تزييف عميق خبيث ومقنع عن طريق الخطأ. ومع ذلك، قد يحاول منشئو التزييف العميق الخبيث الدفاع عن ادعاءات التشهير من خلال القول بأن التزييف العميق هو محاكاة ساخرة إبداعية وليس تمثيلًا مقنعًا للحقيقة في الولايات المتحدة، توفر قوانين التشهير إطارًا قانونيًا يمكن استخدامه لمحاسبة أولئك الذين يستخدمون تقنية التزييف العميق لنشر معلومات كاذبة. في بعض الحالات، قد يقاضي الأفراد أو المؤسسات التي استهدفتها تقنية التزييف العميق منشئي محتوى التزييف العميق بتهمة التشهير ويطالبون بتعويضات في المحكمة. يوفر هذا النهج وسيلة للردع ويمكن أن يساعد في الحد من انتشار تقنية التزييف العميق في الحملات السياسية ووسائل الإعلام. ومع ذلك، من المهم تحقيق التوازن بين حماية حرية التعبير والحاجة إلى منع انتشار المعلومات الكاذبة. ومع تطور تقنية التزييف العميق، ستكون هناك حاجة إلى أساليب أكثر ابتكارًا للكشف عن استخدامها ومنع استخدامها. بشكل عام، من الضروري أن تعمل الوكالات الحكومية وشركات التكنولوجيا وعامة الناس معًا لتعزيز الوعي بالمخاطر التي يشكلها التزييف العميق واتخاذ الخطوات اللازمة لمنع إساءة استخدامه. كانت دعوى التشهير الوحيدة التي ذكرت صراحةً استخدام "التزييف العميق" مرفوعة في يونيو من عام 2021. في هذه الحالة، كان رجل في منتصف العمر يُدعى السيد كوون يترشح لمنصب مجلس إدارة داخل شركته. رفع السيد كوون وشركته دعوى تشهير بعد أن نشر شخص مجهول الهوية صورة "تزييف عميق مُعدل" صور السيد كوون وهو يقبل امرأة أصغر سنًا بكثير. بالنسبة للأفراد

من القطاع الخاص مثل السيد كوون أو الأفراد مثل السيدة مارتن، طبقت المحكمة العليا عددًا أقل من القيود الدستورية.ان الحماية التي توفرها قوانين التشهير لا تقل عن الحماية التي يحصل عليها الشخصيات العامة أو المسؤولون. ففي قضية Gertz v. Robert ، قضت المحكمة العليا بأن الولايات يمكنها أن تحدد معاييرها الخاصة للمسؤولية عن "الأكاذيب التشهيرية الضارة defamatory false-hoods[s‘] بشخص خاص" طالما أن الدولة لا تفرض مسؤولية صارمة عن مثل هذه الأكاذيب. لذلك، في القضايا التي تنطوي على أفراد ليسوا في ضوء عام، سيحتاج المدعون إلى صياغة ادعاءات بعناية لإثبات أن التزييف العميق الخبيث هو تشهيري. هذه مسألة تتعلق بقانون الولاية، وستطبق العديد من العوامل المتعلقة بما إذا كان البيان "كاذبًا حقًا" (وهو ما قد يكون إشكاليًا إذا ذكر الفيديو صراحة أنه مزيف). ومع ذلك، لم يفقد كل الأمل لشخص كان موضوعًا لتزييف عميق خبيث. لقد سنت العديد من الولايات قوانين خاصة بالإباحية غير التوافقية أو "الإباحية الانتقامية" المشابهة لقوانين التشهير. تتضمن الإباحية غير التوافقية توزيع صور جنسية صريحة لأشخاص دون موافقتهم. على الرغم من أن مقاطع الفيديو المزيفة يمكن أن تكون جنسية صريحة، إلا أنها لا تكشف في الواقع عن الهوية الحميمة للضحية ولكنها لا تزال يمكن أن يكون لها نفس التأثيرات المدمرة مثل الفيديو الحقيقي. يعاني الأفراد من الوصمة والعار والإذلال وقد يواجهون صعوبات في تأمين عمل مستقبلي. يجب على الولايات تنظيم الإباحية غير التوافقية لنفس الأسباب التي تنظم بها الإباحية غير التوافقية القياسية. تتمتع الولايات بالسلطة للقيام بذلك منذ أن اعترفت المحكمة العليا، في قضية Miller v. California, rec ، اعترفت المحكمة العليا في قضية ميلر ضد كاليفورنيا بأن المادة الإباحية الأولى المزيفة غير المقبولة هي مادة قانونية. للمزيد ينظر Miller v. California, 413 (U.S. 15 (1973 على موقع المحكمة العليا الامريكية لا/https://supreme.justia.com/cases/federal/us/413/15

[76]ان حقوق التعديل الأول قد تشكل عائقًا كبيرًا أمام ما إذا كان ضحية التزييف العميق الإباحي قادرًا على إنشاء دعوى ضد الجاني بنجاح. وعلى الرغم من أنه من الواضح أن التعديل الأول لا يحمي المواد الفاحشة obscene material، فإن ما إذا كانت المحاكم تعرف المواد الإباحية المزيفة على أنها فاحشة أم لا هو أمر غامض، وخاصة بسبب طبيعتها الحديثة، لذا يعد التعديل الأول للدستور الأمريكي، الذي يحمي حرية التعبير، عقبة رئيسية أمام تجريم المحتوى الإباحي المزيف العميق (Deepfake Pornography)في الولايات المتحدة. التعديل الأول يهدف إلى حماية التعبير، بما في ذلك الصور والفيديوهات، من تدخل الحكومة، مما يجعل القوانين التي تستهدف التزييف العميق تواجه تحديات دستورية. الانه ومع ذلك، تنص القوانين في بعض الولايات على عقوبات معينة في حالات جرائم التزييف العميق المرتبط بالإباحية غير التوافقية من اجل تلافي هذه العقبة، لذا نجد بعض الولايات ، مثل *كاليفورنيا* و*فرجينيا* ، قوانين محددة لمكافحة التزييف العميق الإباحي عن طريق تصنيفها كجريمة في حال استخدامها للإضرار - التهديد - الإكراه. وعلى سبيل المثال، يُعد قانون *كاليفورنيا* لعام 2019 الذي يجرم الإباحية المزيفة غير التوافقية وسيلة قانونية للحد من أضرار هذه التكنولوجيا مع الالتزام بقوانين التعديل الأول، إذ يركز على اضرار الضحية من الجريمة بدلاً من "التعبير ذاته". في حين تقوم ولاية *فيرجينيا* بتوسيع قانون الانتقام الإباحي ليشمل التزييف العميق

الإباحي، مما يجعل توزيع المواد الإباحية المزيفة جريمة إذا كان الهدف " التحرش أو الإكراه"، وذلك ضمن قوانين حماية الخصوصية، للمزيد ينظر في ذلك

Mohamed Chawki, *Ida*. p.9, And see, Timothy Cha, *Federal or State Statutes: Which is the Better Legislative Measure to Combat Deepfake Pornography?* The Department of Engineering and Society, School of Engineering. University of Virginia,2022 p9 on the link file:///C:/Users/SFM/Downloads/3_Cha_Timothy_2022_BS.pdf last seen 1-11-2024.

[77]أن ولايتين فقط، هما فيرجينيا وكاليفورنيا، تدرجان المواد الإباحية المزيفة في قوانين المواد الإباحية الانتقامية

AB California law Article 602 states that "a depicted individual in a pornographic deepfake video has a cause of action against the person who creates and discloses sexually explicit material of this kind." Similarly, Virginia bill HB 2678, passed in 2019, states that the "unlawful [and/or nonconsensual] dissemination or sale of certain images of another person depicted nude or in certain states of undress "constitutes a Class 1 misdemeanor which warrants up to a year of jail or a fine of up to $2,500"

[78] See Matthew F. Ferraro, *Deepfake Legislation: A Nationwide Survey*, WilmerHale Client Alert, September 25, 2019. At 10-12 (discussing Calif. AB-602 and AB-730). And see also, **Jason C. Chipman**, **Stephen W. Preston**, First Federal Legislation on Deepfakes Signed Into Law, **Wilmer Cutler Pickering Hale and Dorr LLP®** DECEMBER 23, 2019. https://www.wilmerhale.com/insights/client-alerts/20191223-first-federal-legislation-on-deepfakes-signed-into-law

[79] الإحصائيات أدناه حتى 31 يوليو لعام 2024 قوانين او مشروعات قوانين تتعلق بالتزييف العميق في الحملات الانتخابية كالتالي: في الولايات المتحدة توجد 19 ولاية سنت قوانين تتناول التزييف العميق والوسائط الخادعة في سياق الانتخابات هذا العام او السنوات الاخيرة، سنت ولاية مينسوتا أول قانون لها بشأن التزييف العميق في عام 2023 وعدلته في عام 2024، وكاليفورنيا قدمت تشريعات قوانين جديدة في عام 2024 حول ذات الموضوع بالاضافة الى قوانين سنتها بين عامي 2019 و2022. وتوجد 6 ولايات سنت قوانين تتعلق بالتزييف العميق في الحملات الانتخابية، ويوجد مايقارب 24 ولاية قدمت مشاريع القوانين بشأن ذات الموضوع في عام 2024 الان انها لن تمرر الى الان. وللمزيد ينظر الدراسة التي تم إعدادها من قبل مركز برينان في أمريكا حول الاتجاهات في مشاريع القوانين المتعلقة بالذكاء الإصطناعي التي قدمتها الولايات المتحدة واقرتها للفترة من (1 يناير ولغاية 31يوليو لعام 2024)

Lewrence Norden,Niyti Narang,Laura J.ida. without noumbers
80 ولاية (ألاباما- اريزونا-كولورادو- هاوي-ميسسبي- نيومكسيكو) سنت قوانين الافصاح مع تقييد الوقت Disclosure laws with time limits في عام 2024 وسبقتها ولاية متشيغان في عام 2023 وكالوفورنيا في 2022، اما ولاية (فلوريدا – ايدوا- انديانا- نيو هامشير- نيويورك – اوريغون- يوتا و وينسكانسن) سنت قوانين الافصاح بدون تقييد للزمان Disclosure laws with no time limits لعام 2024، وسبقتهم ولاية واشنطن في عام 2023، واخيرًا الولايات التي سنت حظر مع حدود زمنية Bans with time limitsولاية تكساس و مينسوتا التي عدلت قانون الافصاح لعام 2022 وحظرت تحديد الزمان في عام 2024 للمزيد ينظر الدراسة التي قدمها مركز برينان للعدالة

Lewrence Norden,Niyti Narang,Laura J. States Take the Lead in Regulation AI in Elections Within Limits, Brennan Center For Justices, published in Augest 7,2024. Last seen 29-2024 on the link below https://www.brennancenter.org/our-work/research-reports/states-take-lead-regulating-ai-elections-within-limits

[81] ولقد فشل المشروعون في بعض الولايات في تمرير قوانين استخدام الذكاء الاصطناعي في شن هجمات على مكاتب الانتخابات والعمليات الانتخابية واستخدام التزييف العميق لخداع العاملين في الانتخابات لحملهم على اتخاذ اجراءات تهدد نزاهة العملية العمليات الانتخابية، وقد نظرت ولايتان على الأقل في توسيع نطاق تنظيم التزييف العميق ليشمل تلك التي تستهدف الإجراءات الرسمية، بما في ذلك الانتخابات. فشل المشرعون في كنتاكي في تمرير مشروع قانون كان من شأنه أن يجرم توزيع "التزييف العميق" الذي "يمكن توقعه بشكل معقول أن يؤثر على سلوك أي إجراء إداري أو تشريعي أو قضائي، بما في ذلك إدارة أو نتيجة الانتخابات" (التأكيد مضاف). كما نظرت ولاية نيوجيرسي في مشروع قانون من شأنه أن يوسع نطاق قانون الاحتيال على الهوية ليشمل "تغيير مناقشة السياسة العامة أو الانتخابات" و "التدخل غير اللائق في إجراء رسمي" باستخدام تقنية التزييف العميق. وقد اقترح المشرعون في ولاية إلينوي مشروع قانون يركز على نطاق أوسع على استخدام "التزييف العميق" لتعطيل الإجراءات الرسمية، والتي من المفترض أن تشمل الانتخابات. ولم يتم تمرير مشروعي القانون في إلينوي ونيوجيرسي بعد للمزيد ينظر https://www.brennancenter.org/our-work/research-reports/states-take-lead-regulating-ai-elections-within-limits وقد أدى القلق الحزبي بشأن التدخل في الانتخابات الناتج عن الذكاء الاصطناعي إلى ظهور مجموعة من القوانين في جميع أنحاء البلاد، حيث يسعى المشرعون في الولايات إلى الحد من تأثير المعلومات المضللة ومنع التزييف العميق من إرهاق الناخبين.

لقد سنت أكثر من اثنتي عشرة ولاية يقودها الجمهوريون والديمقراطيون تشريعات هذا العام لتنظيم استخدام التزييف العميق - مقاطع فيديو وصوت وهمية واقعية ومحتوى آخر تم إنشاؤه باستخدام الذكاء الاصطناعي - في الحملات. تأتي القوانين وسط تحذيرات من وزارة الأمن الداخلي بشأن قدرة التزييف العميق على تضليل الناخبين ومع بقاء الأسئلة حول ما إذا كان الكونجرس قادرًا على اتخاذ إجراءات ذات مغزى قبل نوفمبر 2024 .

لقد أقرت فلوريدا وهاواي ونيويورك وأيداهو وإنديانا ونيو مكسيكو وأوريجون ويوتا وويسكونسن وألاباما وأريزونا وكولورادو قوانين هذا العام تتطلب الإفصاحات في الإعلانات السياسية التي تحتوي على محتوى مزيف عميق. في حين أن ولايات ميشيغان وواشنطن ومينيسوتا وتكساس وكاليفورنيا لديها بالفعل قوانين تنظم التزييف العميق، فقد قامت مينيسوتا بتحديث قانونها هذا العام لإلزام المرشح بالتنازل عن منصبه أو ترشيحه إذا انتهك قوانين التزييف العميق في الولاية، من بين أحكام أخرى. في ولايات مثل نيويورك ونيومكسيكو وألاباما، يمكن للضحايا طلب أمر من المحكمة لوقف المحتوى.

يمكن أن يتلقى منتهكو القوانين المتعلقة بالتزييف العميق في فلوريدا وميسيسيبي ونيومكسيكو وألاباما عقوبة بالسجن. يمكن الحكم على الشخص الذي ينتهك قانون ميسيسيبي بقصد ردع شخص ما عن التصويت أو التحريض على العنف أو الأذى الجسدي بالسجن لمدة أقصاها خمس سنوات، في حين أن العقوبة في فلوريدا هي جنحة من الدرجة الأولى، يعاقب عليها بالسجن لمدة تصل إلى عام واحد.

وقد يؤدي انتهاك القانون أيضًا إلى غرامات باهظة في بعض الولايات: في ولايتي يوتا وويسكونسن، يمكن تغريم المخالفين بما يصل إلى 1000 دولار لكل انتهاك، وفي ولايتي أوريغون وميسيسيبي، يمكن أن تصل الغرامات إلى 10 آلاف دولار

And see, Lewrence Norden,Niyti Narang,Laura J. ida. Without noumbers and see Piper Hudspeth Blackburn, Piper Hudspeth Blackburn, CNNو Wed July 31, 2024 https://edition.cnn.com/2024/07/31/politics/state-laws-election-ai-deepfakes/index.html last seen in 11-12-2024

[82] واقترحت المفوضية الأوروبية المسودة الأولى لقانون الذكاء الاصطناعي في نيسان/أبريل 2021. لكن الدول الأعضاء في الاتحاد الأوروبي كانت مترددة في فرض كثير من القيود على إنفاذ القانون وأمن الحدود، وكانت تخشى من أن يؤدي فرض الكثير من القواعد الروتينية إلى الإضرار بالقدرة التنافسية الاقتصادية. على الرابط التالي اخر زيارة في 1-11-2024
https://www.dw.com/ar/%D8%A7%D9%84%D8%A7%D8%AA%D8%AD%D8%A7%D8%AF-%D8%A7%D9%84%D8%A3%D9%88%D8%B1%D9%88%D8%A8%D9%8A-%D9%8A%D8%B9%D8%AA%D9%85%D8%AF-%D9%82%D8%A7%D9%86%D9%88%D9%86%D8%A7-%D8%B1%D8%A7%D8%A6%D8%AF%D8%A7-%D9%84%D9%84%D8%B0%D9%83%D8%A7%D8%A1-%D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9%D9%8A/a-69140842

[83] Act Intelligence Artificial , European Parliamentary Research Service(EPRS).(2023). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32024R1689

[84] Article 52 of Act Intelligence Artificial

[85] Article 71 – "Penalties and Fines: 1. High-risk AI systems: For providers of high-risk AI systems that fail to comply with the obligations, the fines may reach up to €30 million or 6% of the total worldwide annual turnover, whichever is higher. 2. Incorrect or misleading documentation: If the provider or user provides incorrect, incomplete, or misleading information in documentation, or does not ensure transparency for users, fines may reach €20 million or 4% of the total worldwide annual turnover. 3. Other non-compliances:
For violations that do not fall into high-risk categories, the fines may reach up to €10 million or 2% of the total worldwide annual turnover, whichever is higher.

[86] Article 6 develops this principle by specifying that personal data may not be processed unless there is at least one legal basis for doing so. The other principles refer to "purpose limitation", "data minimization", "accuracy", "storage limitation", and "integrity and confidentiality"."

[87] Article 17 of General Data Protection Regulation (GDPR)2016 provides that," the data subject has the right to request erasure of personal data related to them on any one of a number of grounds, including noncompliance with Article 6(1) (lawfulness) that includes a case (f) if the legitimate interests of the controller are overridden by the interests or fundamental rights and freedoms of the data subject, which require protection of personal data."

[88] Article 5-6-17 of General Data Protection Regulation (GDPR)2016 https://eur-lex.europa.eu/eli/reg/2016/679/oj

[89] Article 82 of the GDPR stipulates that," any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered."

[90] في حكم Österreichische Post (C-300/21) ، قدمت محكمة العدل التابعة للاتحاد الأوروبي تفسيرًا للحق في التعويض. تتطلب المادة 82(1) من اللائحة العامة لحماية البيانات لمنح التعويضات (أ) انتهاك اللائحة العامة لحماية البيانات، (ب) الضرر (الفعلي) الذي لحق به، و(ج) الرابطة السببية بين الانتهاك والضرر الذي لحق به. وليس من الضروري أن يصل الضرر الذي لحق به إلى درجة معينة من الخطورة. ولا يوجد مفهوم أوروبي محدد للضرر.إذ يتم تحديد التعويض على المستوى الوطني وفقًا للقانون الوطني كما يجب مراعاة مبادئ التكافؤ والفعالية تنظر تفاصيل القضية في التقرير المرفق بالرابط ادناه اخر زيارة 2024-11-1 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62021CJ0300

[91] EU Digital Services Act – 2022 on the link https://eur-lex.europa.eu/EN/legal-content/summary/digital-services-act.html

[92] Chesney, Bobby, and Danielle Citron. , *Ida*, 1790. and Vítor Bernardo , *Deepfake detection,EUROPEAN DATA PROTECTIO SUPERVISOR* https://www.edps.europa.eu/data-protection/technology-monitoring/techsonar/deepfake-detection_en last seen in 11-11-2024.

[93]يتم تمرير الصورة عبر شبكة عصبية تقيم الصورة وتستخرج ميزات بسيطة منها. يتم بعد ذلك فحص هذه الميزات بحثًا عن أي تشوهات على
مستوى البكسل والتي يتم تقديمها أثناء إنشاء الصورة المزيفة مثل مخطط الضغط الضائع، والتحف الفنية التي يتم تقديمها أثناء تشويه الصورة والتغييرات الدقيقة في الألوان. للمزيد ينظر
Aarti Karandikar, Vedita Deshpande, Sanjana Singh, Sayali Nagbhidkar, Saurabh Agrawal,Deepfake Video Detection Using Convolutional Neural Network,International Journal of Advanced Trends in Computer Science and Engineering ,Volume 9 No.2, March -April 2020,. p.1313 https://doi.org/10.30534/ijatcse/2020/62922020

[94] Chahal, Prabhjot & Singh, Amritpal & Singh, Palwinder.). Digital Watermarking Techniques. INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY. 11. 2903-2909. 10.24297/ijct.v11i8.3009. (2012) .p.2904. https://www.researchgate.net/publication/324988952_Digital_Watermarking_Techniques

[95] Adi Robertson, *Adobe and Twitter are designing a system for permanently attaching artists' names to pictures* ,The Verge. ,(2019-11-04) on lthe link https://www.theverge.com/2019/11/4/20948229/adobe-twitter-nyt-company-content-authenticity-initiative-attribution-misinformation-tool

[96] Sunkari, Venkateswarlu; Srinagesh, A. Journal of Electrical Systems; Paris Vol. 20, Iss. 5s, (2024): 10-18. P.10 in the link https://www.proquest.com/openview/a08b5fc48939be68905b2c66e2976f78/1?pq-origsite=gscholar&cbl=4433095

[97] علاء الدين منصور مغايرة، مصدر سابق، ص 153.

[98] Anna Maria Collard, *4 ways to future-proof against deepfakes in 2024 and beyond,* Centre for the Fourth Industrial Revolution, Feb 12, 2024 https://www.weforum.org/stories/2024/02/4-ways-to-future-proof-against-deepfakes-in-2024-and-beyond/ last seen 8-11-2024.

المصادر
References

First: Book

I. Pantserev, K.A., *The Malicious Use of AI-Based Deepfake Technology as the New Threat to Psychological Security and Political Stability*. In: Jahankhani, H., Kendzierskyj, S., Chelvachandran, N., Ibarra, J. (eds) Cyber Defence in the Age of AI, Smart Societies and Augmented Humanity. Advanced Sciences and Technologies for Security Applications. Springer, Cham. (2020). (last seen in 3-11-2024) https://doi.org/10.1007/978-3-030-35746-7_3

Second: Legal Research

I. Aarti Karandikar, Vedita Deshpande, Sanjana Singh, Sayali Nagbhidkar, Saurabh Agrawal,Deepfake Video Detection Using Convolutional Neural Network,International Journal of Advanced Trends in Computer Science and Engineering ,Volume 9 No.2, March -April 2020. https://doi.org/10.30534/ijatcse/2020/62922020

II. Ahmed Lotfy El-Sayed Marai, Implications of Artificial Intelligence Technologies on the Theory of Criminal Liability: A Comparative Study, Journal of Legal and Economic Research, Mansoura University - Faculty of Law, Issue 80, 2022, Pages 399-244.

III. Alaa El-Din Mansour Maghareya, Artificial Intelligence Crimes and Ways to Confront Them: Deep Forgery Crimes as a Model, International Journal of Law - Qatar University - Volume 13 - Regular Issue 2, 2024

IV. Ashraf Sayed Abu El-Ela, Criminal Confrontation of Deep Fake Technology, Journal of Legal and Economic Sciences, Issue 66, Issue 3, 2024, Pages 477-511, DOI: 10.21608/jelc.2024.342112.

V. Bobby Chesney Danielle Citron, *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*, California Law Review, Volume 107 , December (2019). in the link https://www.californialawreview.org/print/deep-fakes-a-looming-challenge-for-privacy-democracy-and-national-security

VI. Chahal, Prabhjot & Singh, Amritpal & Singh, Palwinder.). Digital Watermarking Techniques. INTERNATIONAL JOURNAL OF COMPUTERS & TECHNOLOGY. 11. 2903-2909. 10.24297/ijct.v11i8.3009. (2012).

VII. Chesney, Bobby, and Danielle Citron. "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security." *California Law Review* 107, no. 6 (2019): 1753–1820. https://www.jstor.org/stable/26891938

VIII. Claire Langlais-Fontaine: Démêler le vrai du faux: étude de la capacité dudroit actuel à lutter contre les deepfakes, La Revue des droits de l'homme, N°18, 2020. On website https://journals.openedition.org/revdh/9747 last seen 3-10-2024

IX. Edvinas Meskys, Aidas Liaudanskas, Julija Kalpokiene, Paulius Jurcys, Regulating deep fakes: legal and ethical considerations, *Journal of Intellectual Property Law & Practice*, Volume 15, Issue 1, January 2020, Pages 24–31https://doi.org/10.1093/jiplp/jpz167

X. Europol, *Facing reality? Law enforcement and the challenge of deepfakes*, an observatory report from the Europol Innovation Lab, Publications Office of the European Union, Luxembourg.(2022).

XI. Fatih ARSLAN,Deepfake Technology: A Criminological Literature Review,The Sakarya Journal of Law (The SJL), v. 11 section. 1 .p 701-720.p 704. file:///C:/Users/QAA/Downloads/DOC-20240827-

WA0002..pdfhttps://www.researchgate.net/publication/324988952_Digital_Watermarking_Techniques

XII. Ki Chan, C. C., Kumar, V., Delaney, S., & Gochoo, M. (2020). *Combating Deepfakes: Multi-LSTM and Blockchain as Proof of Authenticity for Digital Media.* In 2020 IEEE / ITU International Conference on Artificial Intelligence for Good, AI4G 2020 (pp. 55-62). Article 9311067 (2020 IEEE / ITU International Conference on Artificial Intelligence for Good, AI4G 2020). Institute of Electrical and Electronics Engineers Inc.. https://doi.org/10.1109/AI4G50087.2020.9311067

XIII. Mahmoud Salama Abdel Moneim El-Sherif, The Crime of Revenge Pornography Through Deep Forgery Technology and Criminal Liability for It, Journal of Law for Legal and Economic Research, Alexandria University, Volume 5, Issue 1, 2022, pp. 366-485. On the link, https://lalexu.journals.ekb.eg/article_266089.html . last seen in 2024-10-27.

XIV. Mariëtte van Huijstee , Pieter van Boheemen ,Djurre Das and etal., Tackling deepfakes in European policy, Panel for the Future of Science and Technology, European Parliamentary Research Service, Scientific Foresight Unit (STOA), PE 690.039 – July 2021.

XV. Matthew B. Kugler and Carly Pace, *Deepfake Privacy: Attitudes and Regulation*, 116 Nw. U. L. Rev. 611 (2021). https://scholarlycommons.law.northwestern.edu/nulr/vol116/iss3/1

XVI. Meskys, Edvinas and Kalpokiene, Julija and Jurcys, Paul and Liaudanskas, Aidas, *Regulating Deep Fakes*: Legal and Ethical Considerations (December 2, 2019). Journal of Intellectual Property Law & Practice, Volume 15, Issue 1, January 2020,

Pages 24–31., Available at SSRN: https://ssrn.com/abstract=3497144 _

XVII. Mohamed Chawki (2024) Navigating legal challenges of deepfakes in the American context: a call to action, Cogent Engineering, 11:1, 2320971, DOI: 10.1080/23311916.2024.2320971

XVIII. Sandeep Singh Mankoo. "DeepFakes- The Digital Threat in the Real World." Gyan Management Journal 17/1 (2023), 71-77. https://doi.org/10.48165/gmj.2022.17.1.8

XIX. Sunkari, Venkateswarlu; Srinagesh, A. Journal of Electrical Systems; Paris Vol. 20, Iss. 5s, (2024): 10-18. P.10 in the link https://www.proquest.com/openview/a08b5fc48939be68905b2c66e2976f78/1?pq-origsite=gscholar&cbl=4433095

XX. Timothy Cha, Federal or State Statutes: Which is the Better Legislative Measure to Combat Deepfake Pornography? The Department of Engineering and Society, School of Engineering. University of Virginia,2022. on the link file:///C:/Users/SFM/Downloads/3_Cha_Timothy_2022_BS.pdf last seen 1-11-2024.

XXI. Vig, Shinu. "*Regulating Deepfakes: An Indian perspective*." Journal of Strategic Security 17, no. 3 (2024) : 70-93.DOI: https://doi.org/10.5038/1944-0472.17.3.2245 Available at: https://digitalcommons.usf.edu/jss/vol17/iss3/5

Third: Thesies

I. S. Bates, '"*Stripped": An Analysis of Revenge Porn Victims' Lives after Victimization'*, Thesis Submitted in Partial Fulfillment of the Requirements for the Degree of Master of Arts/ SIMON FRASER UNIVERSITY. 2012. (available at: https://summit.sfu.ca/item/15668)

Forth: Articles

I. Abdullah bin Hussein Al-Asmari, Deep Forgery Technology and Artificial Intelligence, Ministry of the National Guard - Saudi Arabia, 5-25-2023, on the link https://kkmag.sang.gov.sa/Technicalarticles/Pages/%D8%AA%D9%82%D9%86%D9%8A%D8%A9-%D8%A7%D9%84%D8%AA%D8%B2%D9%8A%D9%8A%D9%81-%D8%A7%D9%84%D8%B9%D9%85%D9%8A%D9%82-%D9%88%D8%A7%D9%84%D8%B0%D9%83%D8%A7%D8%A1-%D8%A7%D9%84%D8%A7%D8%B5%D8%B7%D9%86%D8%A7%D8%B9%D9%8A.aspx

II. Adi Robertson, 3- Adobe and Twitter are designing a system for permanently attaching artists' names to pictures ,The Verge. ,(2019-11-04) on lthe link https://www.theverge.com/2019/11/4/20948229/adobe-twitter-nyt-company-content-authenticity-initiative-attribution-misinformation-tool

III. Ambrose, T. UK's enemies could use AI deepfakes to try to rig election, says James Cleverly. (2024, February 25). . The Guardian. https://www.theguardian.com/uk-news/2024/feb/25/uks-enemies-could-use-ai-deepfakes-to-try-to-rig-election-says-james-cleverly

IV. Anna Maria Collard, *4 ways to future-proof against deepfakes in 2024 and beyond*, Centre for the Fourth Industrial Revolution, Feb 12, 2024 https://www.weforum.org/stories/2024/02/4-ways-to-future-proof-against-deepfakes-in-2024-and-beyond/ last seen 8-11-2024.

V. Durbin, R. J., & Graham, L., The DEFIANCE Act of 2024. https://www.durbin.senate.gov/imo/media/doc/defiance_act_of_2024.pdf

VI. EM Ellis, '*People Can Put Your Face on Porn—and the Law Can't Help You'*, (available at: https://www.wired.com/story/face-swap-porn-legal-limbo) .

VII. EM Ellis, 'People Can Put Your Face on Porn—and the Law Can't Help You', (available at: https://www.wired.com/story/face-swap-porn-legal-limbo).

VIII. Emily Hallas, How battleground states are targeting AI and 'deepfakes' in

IX. Europol , Facing reality? Law enforcement and the challenge of deepfakes, an observatory report from the Europol Innovation Lab, Publications Office of the European Union, Luxembourg.(2022).

X. Geller, E., & Vinocur, N. (2017, May 5). French presidential candidate confirms 'massive' hack days before election. Politico. https://www.politico.com/story/2017/05/05/emmanuel-macron-french-election-hack-cyber-238059

XI. **Jason C. Chipman**, **Stephen W. Preston**, First Federal Legislation on Deepfakes Signed Into Law, **Wilmer Cutler Pickering Hale and Dorr LLP®** DECEMBER 23, 2019. https://www.wilmerhale.com/insights/client-alerts/20191223-first-federal-legislation-on-deepfakes-signed-into-law

XII. Lewrence Norden,Niyti Narang,Laura J. States Take the Lead in Regulation AI in Elections Within Limits, Brennan Center For Justices, published in Augest 7,2024. Last seen 29-2024 on the link below https://www.brennancenter.org/our-

work/research-reports/states-take-lead-regulating-ai-elections-within-limits

XIII. Matthew F. Ferraro, Deepfake Legislation: A Nationwide Survey, WilmerHale Client Alert, September 25, 2019. At 10-12 (discussing Calif. AB-602 and AB-730)

XIV. Oliver Lock , *Artificial Intelligence Guidance on Lexis+*,Produced in partnership with Oliver Lock of Farrer & Co,2024, https://www.lexisnexis.co.uk/legal/guidance/deepfakes last seen in 11-11-2024

XV. P Hayward, A Rahn, 'Opening Pandora's Box: pleasure, consent and consequence in the production and circulation of celebrity sex videos' (2015) 2(1) Porn Studies 49 . https://doi.org/10.1080/23268743.2014.984951

XVI. Piper Hudspeth Blackburn, Piper Hudspeth Blackburn, CNNو Wed July 31, 2024 https://edition.cnn.com/2024/07/31/politics/state-laws-election-ai-deepfakes/index.html.

XVII. RESEARCH PROJECT ,*Misinformation and Misinformation and Deepfakes*,on the website of university of Essex/Human Rights Big Data and Technology Law Enforcement. (without name and date) last seen in 11-11-2024 . https://www.essex.ac.uk/research-projects/human-rights-big-data-and-technology/misinformation-and-disinformation-and-deep-fakes

XVIII. Şeymanur Yönt, *The Deepfake Menace: Legal Challenges in the Age of AI*, TRT TRAINING AND RESEARCH DEPARTMENT ,March 2024,p6. Last seen in 5-10=2024 on file:///C:/Users/QAA/Downloads/The-Deepfake-Menace_v2.pdf

XIX. Terrence Matsuo, Deepfakes and Korean Society: Navigating Risks and Dilemmas,October 3, 2024

XX. Vincent, J. Watch Jordan Peele use AI to make Barack Obama deliver a PSA about fake news. (2018, April 17). The Verge. https://www.theverge.com/tldr/2018/4/17/17247334/ai-fake-news-video-barack-obama-jordan-peele-buzzfeed

XXI. Vítor Bernardo , Deepfake detection,EUROPEAN DATA PROTECTION SUPERVISOR, https://www.edps.europa.eu/data-protection/technology-monitoring/techsonar/deepfake-detection_en

XXII. Weatherbad, J. *Trolls have flooded X with graphic Taylor Swift AI fakes*. , January, 2024. The Verge. https://www.theverge.com/2024/1/25/24050334/x-twitter-taylor-swift-ai-fake-images-trending