Journal Of the Iraqia University (75-3) February (2026)

ISSN(Print): 1813-4521 OnLine ISSN:2663-7502

Journal Of the Iraqia University

available online at

https://iasj.rdd.edu.iq/journals/journal/view/247

التزييف العميق كجريمة رقمية مركبةتحليل قانوني للمخاطر الأمنية والقانونية في البيئة الرقمية

م. د. حسين عباس حميد

كلية القانون/ جامعة الفراهيدي

Deepfake as a Complex Cybercrime: A Legal Analysis of Security and Legal Risks in the Digital Environment

Asst. Prof. Dr. Hussein Abbas Hameed

Hussein.abbas1994@gmail.com

ملخص البحث:

يُعد التزييف العميق (Deepfake) من ضمن المخاطر الكبيرة التي أفرزتها تقنيات الذكاء الاصطناعي التوليدي في الشق الرقمية، حيث يتيح إنشاء محتوى مرئي أو صوتي مزيف يحاكي الواقع بدرجة عالية من الدقة، هذا التطور التقني ساهم في تحويل التزييف العميق من مجرد أداة ترفيه إلى سلاح رقمي يُستخدم في ارتكاب جرائم معقدة تمس الأمن القومي، والنظام العام، وحقوق الأفراد، ما يجعله جريمة رقمية مركبة تتقاطع فيها عدة أنماط إجرامية كالتزوير، الاحتيال، التشهير، وانتهاك الخصوصية.يتناول هذا البحث الأبعاد الأمنية والقانونية للتزييف العميق، ويحلل أوجه القصور في التشريعات التقليدية، مع التركيز على البيئة التشريعية التي وجدت لديها آلية للتصدي، كما يستعرض البحث التحديات التي تحيط بسلطات التحقيق والجهات القضائية لإثبات هذا النوع من الجرائم، ويقترح حلولًا تشريعية وتقنية للحد من مخاطره، ويخلص إلى ضرورة وضع ثوابت تشريعية خاصة تواكب التطور في ارتكاب جرائم تقنية المعلومات، إلى جانب تعزيز الجوانب الفنية والعملية للتصدي لهذه الظواهر الاجرامية المتسارعة. **الكلمات المفتاحية:** التزييف العميق، الذكاء الاصطناعي، الأمن الرقمي، المسؤولية الجنائية، الخصوصية، الأدلة الرقمية.

Abstract:

Deepfake technology is one of the major risks introduced by generative artificial intelligence in the digital realm. It enables the creation of highly realistic fake visual or audio content that closely mimics reality. This technological advancement has transformed deepfakes from mere entertainment tools into digital weapons used in the commission of complex crimes that threaten national security, public order, and individual rights. As such, deepfakes constitute a **composite cybercrime**, intersecting with various criminal patterns such as forgery, fraud, defamation, and privacy violations.This research examines the **security and legal dimensions** of deepfake technology, analyzes the shortcomings of traditional legislation in addressing such crimes, and highlights legislative environments that have developed mechanisms to confront them. It also explores the challenges faced by investigative authorities and judicial bodies in proving these types of offenses. The study proposes both legislative and technological solutions to mitigate the risks posed by deepfakes, emphasizing the urgent need for **dedicated legal frameworks** that keep pace with the evolution of cybercrime. Additionally, it calls for strengthening technical and procedural capabilities to effectively counter this rapidly emerging criminal phenomenon.**Keywords**: Deepfake, Artificial Intelligence, Digital Security, Criminal Liability, Privacy, Digital Evidence

مقدمة

مع ازدياد تنامي استخدام تقنيات الذكاء الاصطناعي في شتى مجالات الحياة، ظهرت تطبيقات متقدمة باتت تمثل تهديدًا مباشرًا للثقة الرقمية، من أبرزها تقنية التزييف العميق (Deepfake)، التي تقوم على استخدام خوارزميات التعلم العميق لإنشاء محتوى مرئي أو صوتي مزيف يبدو واقعيًا بدرجة يصعب معها التمييز بين الحقيقي والمفبرك، ورغم تطويع هذه التقنية في بعض الاستخدامات المشروعة، فإنها سرعان ما تحولت إلى أداة

رقمية تُستغل في تنفيذ جرائم معقدة ذات أبعاد أمنية وقانونية بالغة الخطورة.ويكمن جوهر التهديد في الطابع المزدوج لهذه الجريمة؛ فهي لا تقتصر على فعل تزوير المحتوى فحسب، بل قد تتداخل مع عدة جرائم رقمية أخرى، مثل الابتزاز الإلكتروني، وانتهاك الخصوصية، وانتحال الهوية، والتحريض على العنف أو التشهير، فضلًا عن تهديد الأمن القومي والتأثير على الرأي العام، وبالتالي، فإن التزييف العميق لا يُعد مجرد مظهر من مظاهر الجريمة الرقمية، بل منصة رقمية متعددة الأبعاد تُستخدم لتنفيذ أفعال جنائية مركبة يصعب تتبعها أو إثباتها باستخدام الأدوات التقليدية.وإزاء هذه التحديات، يواجه النظام القانوني أزمة حقيقية في تكييف هذه الأفعال، سواء على مستوى التشريعات الوطنية منها العراق التي قد تعاني من فراغ أو غموض تشريعي، أو على مستوى آليات التحقيق والإثبات الرقمي، كما يفرض التزييف العميق تحديات أمنية تتعلق بكيفية رصد هذه المواد المزيفة قبل انتشارها، وحماية الأفراد والكيانات من آثارها المدمرة.وانطلاقًا من ذلك، تهدف هذه الدراسة إلى تقديم تحليل قانوني ممنهج للتزييف العميق كجريمة رقمية مركبة، من خلال:

١.تحديد الطبيعة القانونية للتزييف العميق في ضوء القواعد العامة لجرائم تقنية المعلومات.

٢.تحليل صور وأركان الجرائم المرتكبة.

٣.استعراض المخاطر الأمنية المرتبطة به.

٤.تقييم مدى كفاية المصدات التشريعية النافذة للتصدي.

٥.اقتراح حلول تشريعية وإجرائية فعّالة لمواكبة هذا التحدي التقني الخطير.

وتستند هذه الدراسة إلى منهج تحليلي نقدي مقارن، يأخذ بالتصور اعتبارات التطور في الجانب التقني والتشريعي على المستويين الوطني والدولي، ويهدف إلى بناء رؤية متكاملة للمواجهة بعدّ ان الجريمة معقدة خاصة وهو تنشأ في بيئة رقمية مختلفة عن الجريمة التقليدية.

خطة الدراسة:

المبحث الأول: التزييف العميق كفعل جنائي رقمي المطلب الأول: الإطار النظري لفعل التزييف العميق المطلب الثاني: التكييف الجنائي للتزييف العميق المبحث الثاني: التهديدات الأمنية والقانونية للتزييف العميق المطلب الأول: التأثير الأمني للتزييف العميق على النظم السياسية والمجتمعية.المطلب الثاني: الانتهاكات الناجمة عن التزييف العميق.

المبحث الأول التزييف العميق كفعل جنائي رقمي

إن التزييف العميق (Deepfake) يُعد من أبرز الأخطار الجزائية الافتراضية الناشئة عن توظيف تقنيات الذكاء الاصطناعي في إنتاج محتوى وهمي، يُظهر أشخاصًا حقيقيين وهم يرتكبون أفعالًا لم يقوموا بها، أو يقولون ما لم يصرّحوا به، وذلك بدقة عالية تجعل من التمييز بين الحقيقي والمزيّف أمرًا بالغ الصعوبة حتى على الخبراء.إذ تتمثل الخطورة الجنائية للتزييف العميق بكونه أداة فاعلة بل بارزة في ارتكاب عدد من الجرائم الرقمية، منها انتحال الشخصية عبر إنشاء مقاطع صوتية أو مرئية مزيفة بهدف الخداع أو الاحتيال، او جرائم مثل الابتزاز الإلكتروني من خلال تركيب مشاهد مخلة أو مهينة لأشخاص حقيقيين وتهديدهم بنشرها، او حتى جريمة تحريض على ارتكاب العنف أو أفعال الكراهية عن طريق نسب أقوال أو أفعال لأشخاص عامين تثير الفتن أو تضر بالأمن العام، او الترويج للأخبار غير الدقيقة واستمالة الرأي العام له خاصة في مواقيت الانتخابات أو الأزمات التي تمر بها البلدان، ويمكن ايضًا استخدامها في الإضرار بالسمعة وتشويه الصورة، وهي جرائم قد تدخل ضمن إطار التشهير أو الإضرار العمدي بالغير، إذ يُصنف التزييف العميق ضمن الأفعال الجنائية الرقمية المعقدة، نظرًا لعدة عوامل، منها صعوبة التحقق من المصدر الأصلي للفيديو أو الصوت، والقدرة على إنتاج محتوى يصعب كشف زيفه إلا باستخدام أدوات تحليل متقدمة، والانتشار السريع للمحتوى على منصات التواصل الاجتماعي قبل التحقق منه.ومن أجل ذلك، يقتضي الأمر ضرورة تحديث الأطر القانونية التقليدية لتشمل هذا النوع من الأفعال، سواء من خلال تكييفها كجرائم قائمة كالتزوير، الاحتيال، أو التشهير، أو النص على تجريمها بصورة مستقلة ضمن قوانين الجرائم التي تكافح جرائم تقنية المعلومات.

المطلب الأول الإطار النظري لفعل التزييف العميق

إن التزييف العميق يعد اليوم من أكبر بل وأخطر ما انتجته التقنية خاصة وانه يستخدم في العديد من الأفعال الخطرة، والتي تستهدف الحياة الخاصة للأفراد، من خلال انشاء محتوى رقمي مزيف سواء كان صوتيًا أو صوريًا أو فيديويًا، وهذه التقنية بهذا الحجم من الخطورة تهدد بصورة كبيرة حياة الأفراد وخصوصيتهم، كما من البين بأن هذه العمليات تعزز تآكل الثقة بالمحتوى الرقمي بصورة كبيرة.على المستوى التطبيقي ان تقنية التزييف العميق عملية يمكن من خلالها ان تجمع مجموعة من الصور او الفيديوهات أو الأصوات لأحد المستخدمين، ومن خلال أدوات للذكاء

الاصطناعي تدخل هذه البيانات الشخصية من أجل أن يتعرف عليها ويتعلم منها كيف يتحرك ويتكلم ذلك الشخص، وفي خطوة لاحقة يقوم بعملية توليد الفيديو أو الصوت فتجعل ذلك الشخص يتحرك ويقول ما يريد الشخص المستخدم لهذي التقنية بصورة طبيعية بصورة عالية الدقة والمخاطر، ومن البين الواضح ان الأمر يتطور بصورة فائقة، إذ تمكّن هذه التقنية إمكانية إنشاء أصوات وفيديوهات لأي شخص حقيقي أو حتى افتراضي يقول أو يفعل أشياء لم يفعلها مطلقًا، مما قد تتسبب هذه التقنية في الاضرار بالخصوصية كسرقة الهوية الشخصية أو الحصول على منفعة مالية أو معنوية، كما يمكن ان تشكل هذي التقنية مخاطر أخرى مثل جعل شخص في موضع التأييد لفكرة أو منتج، وقد يذهب لأبعد من ذلك بجعل الموظف العام يتقاضى رشاوي باستخدام التزييف العميق (ريم غريب الشامسي ، ٢٠٢٢: ٢٩)إضافة لذلك إن تقنية التزييف العميق هي التقنية التي تستخدم منهجية التعلم العميق التي تُعد إحدى مكونات الذكاء الاصطناعي، يهدف من خلاله عمل محاكاة غير حقيقية لموقف أو تصرف لشخص تبدو وكأنها حقيقية، ولكنها لسيت كذلك، ويأتي مصطلح deep من فكرة التعلم وfake من فكرة الخداع والتزوير، في حين إن مصطلح التزييف العميق بذاته يُعد عملية جمع ملفات الصوت أو الفيديو بواسطة الذكاء الاصطناعي أو التعلم الآلي بصورة دقيقة، وتكون مجالات افعال التزييف العميق مبتدئة من عمليات استبدال الوجوه أو عملية تحريك الشفاه اذ يمكن وضع فم المتحدث ينطق كلمات احترافية أي وضعه على ملف صوت غير الشخص الحقيقي أي انه مختلف عن الصوت الأصلي او عملية وضع نسخة أخرى من الصوت (د. سامح محمد محمد السيد إبراهيم، ، ٢٠٢٥: ٣٩٦٦)ومن خلال الدراسة وجد الباحث إن هنالك بعض من التشريعات عرفت هذه التقنية Deepfakes بأنها مشهد فيديوي ينشأ لغرض الخداع، يصور على انه حقيقي لشخص يقوم بعمل لم يكن حقيقًا (S.B. No. 751, AN ACT,)وإشارة لما ذكر فان ولاية كاليفورنيا سارت نحو النص صراحة بحظر استخدام هذه التقنية في مجال التصدي لهذه الجريمة وخاصة في أوقات الانتخابات، من خلال عدم إجازة للشخص أو اللجنة، أو أي كيان في غضون ٦٠ يومًا من الانتخابات التي سيظهر فيها مرشح للمنصب الانتخابي في الاقتراع، ويوزع بسوء نية، وسائط صوتية أو بصرية خادعة ماديًا، للمرشح بقصد الاضرار بسمعة المرشح أو خداع ناخب للتصويت لصالح المرشح أو ضده (Cal. Elec. § 20010)كما نجد إن تقنية التزييف العميق عرفت بانها مشهد فيديوي يكون القصد من إنشاؤه خداع الاشخاص، ويظهر على انه شخصًا حقيقيًا يتصرف تصرفات لم تحدث في الواقع، كما يمكن تعريف التزييف العميق على انه محتوى مرئي أو صوتي أو كلاهما تم التلاعب به باستخدام الذكاء الاصطناعي وتقنية برمجيات متقدمة لتزييف حقيقة الأفراد والأشياء والأماكن والأحداث، ويبدو هذا المحتوى المزيف قريبًا من الواقع، وقد يجد عامة الناس صعوبة في اكتشافه (دليل التزييف العميق، ٢٠٢١: ٥)ومن خلال تحليل النصوص التي جاءت بها التشريعات وخاصة في الولايات المتحدة في الامريكية بانها من قبيل التشريعات أو النصوص الخاصة بموضوع معين ألا وهو الموضوع الانتخابي، إذ أنها لا تجرم هذه التقنية بذاتها أو لخطرها إلا بما يتعلق باستغلالها في الموضوعات الانتخابية، على أنها وسيلة أو أداة تستعمل في ارتكاب الجريمة.وحين التطرق للتشريعات العربية نجد إن المشرع المصري نص بين ثنايا قانون رقم ١٧٥ لسنة ٢٠١٨ الخاص بمكافحة جرائم تقنية المعلومات في مادته الـ ٢٦ بانه "يعاقب بالحبس مدة لا تقل عن سنتين وبغرامة لا تقل عن مائة ألف جنيه ولا تجاوز ثلاثمائة ألف جنيه أو بإحدى هاتين العقوبتين كل شخص تعمد استعمال برنامج معلوماتي أو تقنية معلوماتية في معالجة معطيات شخصية للغير لربطها بمحتوى منافٍ للآداب العامة، أو لإظهارها بطريقة من شأنها المساس باعتباره أو شرفه".ونشير إلى إن القانون في مصر لم يشر صراحة لتعريف هذه التقنية أو أن يذكر تقنية التزييف العميق بصورة صريحة، إلا إن النص من وجهة نظر الباحث يستوعب هذه التقنية من خلال ذكر استخدام التطبيق الرقمي أو تقنية المعلومات من أجل المعالجة لهذه المعطيات الذاتية للأشخاص التي تنتج بالنهاية لوضع الشخص بموضع غير لائق أو محالف للآداب العامة (حسين عباس حميد، ، ٢٠٢٤: ١٧٣) ومن أجل الدراسة يمكن للباحث أن يعرف تقنية التزييف العميق بإنها (هي تلك العمليات أو الاستخدامات لتطبيقات الذكاء الاصطناعي التي تهدف لإنشاء محتوى رقمي، سواء كان صوتيًا أو مرئيًا أو كتابيًا، يُنسب إلى شخص لم يقم به فعليًا، أو يُحاكي حدثًا لم يقع في الواقع).

المطلب الثاني التكييف الجنائي للتزييف العميق

إن التطور المتسارع في تطبيقات الذكاء أدى لتنامي ظواهر حديثة تحمل أبعاد قانونية معقدة، من أبرزها تقنية التزييف العميق (Deepfake)، التي تقوم على إنشاء محتوى مرئي أو صوتي مزيّف عالي الدقة يصعب تمييزه عن الحقيقي، وقد تجاوزت آثار هذه التقنية الجوانب التقنية والفنية لتثير إشكالات خطيرة في المجال الجنائي، نظراً لقدرتها على خداع الحواس، وانتحال الصفات، والمساس بحرمة الحياة الخاصة، بل وحتى تقويض الثقة بالأدلة الرقمية والشخصيات العامة.إن التحدي الأساسي الذي يفرضه التزييف العميق على القانون الجنائي يتمثل في إيجاد تكييف قانوني دقيق ومناسب لهذا السلوك، يُمكِّن من مساءلة مرتكبيه جنائياً وفق القواعد العامة أو من خلال نصوص قانونية خاصة. ويستدعي ذلك تحليل

البنية الفنية للتزييف العميق، وتحديد عناصره المادية والمعنوية، ومقارنته بالجرائم التقليدية المشابهة كجريمة التزوير، أو القذف، أو نشر المحتوى الإباحي، أو المساس بأمن الدولة، فضلاً عن استجلاء الموقف التشريعي من هذه التقنية في ظل غياب أو حتى قصور بعض القوانين عن مواكبة المستجدات الرقمية.بما ان روبوتات الذكاء الاصطناعي وبرامجه باتت اليوم تستخدم لدى مجموعة واسعة من التطبيقات، مثلا في الصناعة او الخدمات العسكرية وفي الخدمات الطبية وحتى العلوم، وغيرها من المجالات ذات الصلة، ولفرض المسؤولية الجنائية بات التفكير يتجه نحو إمكانية توقيع الجزاء الجنائي على هذه الكيانات وتحديد قواعد فرضها، أي انه هل من الضروري ان يقع على عاتق الذكاء الاصطناعي المسؤولية الجنائية عما يرتكبه من افعاله الاجرامية، فمن أجل فرض المسؤولية في المجال الجنائي بحق الأشخاص من المهم ملاحظة أنه لا بد من ان يتوفر لدى فعله عنصران رئيسيان يتمثل الأول في العنصر الخارجي أي السلوك الاجرامي وهو ما يسمى بالركن المادي والثاني العنصر الداخلي او النفسي وهو ما يطلق عليه الركن المعنوي (بن عودة حسكر مراد، ، ٢٠٢٢: ١٩٧) . تكون الجريمة عمدية وفقًا لقانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ وتعديلاته إذا توافر القصد الجرمي، إذ تفترض المسؤولية الجنائية ثبوت الفعل للفاعل ونسبة النتيجة إلى الفعل، استنادًا إلى نظرية تعادل الأسباب، والسبب الكافي لربط الفعل بالنتيجة، ومن هذا يجب ان نبين بانه هذا ما لا يمكن توقعه إلا في حال وجود الإرادة المستقلة لدى الفاعل ويكون الشخص يمتلك القدرة قادرًا على التمييز والادراك، وهذا الأمر ما لا نجده إلا في الشخص الطبيعي، فالإنسان وحده يكون أهلًا لتحمل هذه المسؤولية (محمد عباس حمودي حسين الزبيدي ونور قيس محمد شاهين، ٢٠٢٤: ٢٩) . وهذا الرأي يمكن أن يفند، خاصة من خلال ما أُرفد للشخص المعنوي من مسؤولية جنائية (قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ وتعديلاته في المادة ٨٠) ، ويمكن أن يقاس عليه ذلك فيما يمكن للذكاء الاصطناعي أن يفعله وخاصة مع ما وصل اليه من تطور كبير من فهم وإدراك اصطناعي، إذ بات اليوم يقدّر افعاله بصورة يمكن من خلاله ان يفهم الفعل الذي يشكل جريمة من عدمه.ومن زاوية أخرى لا بُدَّ من الإشارة إلى أن معالجة المعطيات الشخصية في العديد من التشريعات تعد جرائم في حالة تم إساءة استعمال هذه المعطيات، وخاصة في ارتكاب أفعال منافية للأخلاق أو الآداب العامة.ونجد إن المشرع المصري قد أشار لذلك من خلال النص صراحة في المادة ٢٦ من قانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات (قانون رقم ١٧٥ لسنة ٢٠١٨ ، العدد ٣٢ مكرر (ج) ٢٠١٨) ، إذ بينت المادة ماهية السلوك بواسطة استخدام البرنامج المعلوماتي أو التطبيقات التقنية من اجل المعالجة الخاصة بالمعطيات الخاصة بالأشخاص من اجل تكاملها ونشرها بمحتوى مناف للآداب العامة، أو من اجل إظهارها بطريقة بشأنها ان تمس اعتباره او شرفه، في حين إن الركن المعنوي يتمثل في أن يتوافر القصد الجرمي لدى مرتكب هذه الجريمة حتى تكتمل مكوناتها القانونية، وهو لن يكون كذلك ما لم تتجه إرادة الجاني الى ارتكاب العناصر المكونة للجريمة وتوافر علمه بذلك، اذ يجب ان تتجه الإرادة المعتبرة قانونًا الى معالجة المعطيات الشخصية للمجني عليه لربطها بمحتوى مناف للآداب العامة أو لإظهار هذه المعطيات بطريقة من شأنها المساس باعتبار او شرف المجني عليه (احمد عبد الموجود أبو الحمد زكير، ٢٠٢٢، ٢٢٨٠).ومن خلال ذلك، نجد ان التكييف الجنائي لهذا النوع من الجرائم يعتمد بصورة أساس على البيانات الشخصية، وما تشكله من أهمية كبيرة في استخدام هذه التطبيقات لارتكاب هذه الأفعال الجرمية، والتي تمس الحياة الخاصة للأفراد او المؤسسات او الشخصية المعترف بها قانونيًا، وكذلك تشكل البيانات الشخصية القيمة العُليا في أي جريمة يستخدمها الذكاء الاصطناعي بذاته، إذ ان معالجة البيانات ومن ثم تحليلها ووضعها في صورة سلوك جرمي.

المبحث الثاني التهديدات الأمنية والقانونية للتزييف العميق

إن ما يشهد العالم من تطور متسارع في تقنيات الذكاء الاصطناعي، ومن أبرز هذه التقنيات ما يُعرف بالتزييف العميق (Deepfake)، وهي تقنية تقوم على استخدام خوارزميات الذكاء الاصطناعي، لا سيما شبكات التعلّم العميق (Deep Learning)، لإنشاء محتوى مرئي أو صوتي مزيف يبدو واقعيًا بدرجة يصعب معها التمييز بين الحقيقي والمفبرك.وعلى الرغم من الاستخدامات الكثيرة الإيجابية لهذه التقنية في مجالات مثل السينما والتعليم وغيرها من المجالات، إلا أن مخاطرها الأمنية والقانونية باتت تتصدر المشهد التقني، فقد بات بالإمكان استعمال التقنية لتزوير المشاهد الفيديوية لشخصيات عامة أو مسؤولي دول، ونشر أخبار كاذبة، أو انتحال الشخصية، أو ارتكاب جرائم إلكترونية معقدة، مما يشكل تهديدًا مباشرًا للأمن القومي، ويقوّض الثقة في وسائل الإعلام، ويخلق بيئة خصبة لابتزاز الأفراد والمؤسسات.ومن الاتجاه القانوني، يطرح هذا النوع من التطبيقات إشكالية معقدة تتعلق بإثبات الجريمة، وتحديد المسؤولية الجنائية، وتكييف الأفعال في ضوء التشريعات القائمة التي قد تكون عاجزة عن مواكبة هذه الظواهر التقنية المعاصرة.لذلك، باتت هنالك ضرورة كبيرة لدراسة هذه المهددات بصورة معمقة، من خلال تحليل الأبعاد القانونية والأمنية للتزييف العميق، واستعراض الجهود التشريعية الدولية والوطنية للتصدي لها، واقتراح حلول توازن بين التطور التكنولوجي وحماية الحقوق الأساسية.

المطلب الأول التأثير الأمني للتزييف العميق على النظم السياسية والمجتمعية

إن تطوير الذكاء الاصطناعي أدى لزيادة في مخاطر التزييف العميق بصورة كبيرة، إذ يمكن للخوارزميات من إنشاء وسائط يصعب تمييزها عن الصور الحقيقة أو مقاطع الفيديو أو التسجيلات الصوتية، علاوة على ذلك، يمكن الحصول على هذه الخوارزميات بتكلفة منخفضة، ويمكن إدراج عدد لا كبير من المعطيات بما يمكن التوصل بسهولة اليها، مما يسهل على مجرمي الإنترنت إنشاء عمليات تزوير عميقة تمكنهم من صنع هجمات احتيالية على الأفراد أو المؤسسات (الذكاء الاصطناعي ومخاطر التزييف العميق، ٢٠٢٣) . إن التقنية الحديثة باتت اليوم تمثل أدوار كبيرة في نشر الفوضى بسبب بعدم وجود اطر قانونية وتنظيمية محددة لهذه التطبيقات، فمنها نشر الفوضى او الاشاعات او الأكاذيب، من خلال تطبيقات التواصل الاجتماعي.إن تقنية الذكاء الاصطناعي تلعب ادوارًا خطرة في نشر الشائعات والأكاذيب، بهدف تقويض استقرار الدول، واسقاط الأنظمة، وبث الفوضى في العديد من مناطق العالم، وقد تحولت هذه التطبيقات بالفعل بالأوقات القليلة الماضية ليصبح الرافد الرئيس لصناعة ما يسمى بالكذب أي المنافي للحقيقة، وهو نوع جديد من التصورات المنافية للحقيقة، باستطاعته ان ينتج الصور الثابتة وكذلك المتحركة ومشاهد تشابه الواقع والحقيقة، وتؤثر على أمن واستقرار الدول (سامح محمد محمد السيد ابراهيم، ٢٠٢٥، ٣٩٧٤)كما يمكن استخدام هذه التقنية لصناعة فيديوهات للانتقام من الأشخاص، والمعروف ايضًا باسم الانتقام الاباحي، وهي من جرائم العنف الجنسي عبر الإنترنت، إذ يقصد به نشر صور عارية أو مقاطع فيديو جنسية لشخص ما، بصورة صريحة على الإنترنت، عدة ما تتم عن طريق شريك جنسي سابق، دون موافقة الشخص المعني، ومن أجل التسبب في الضيق او الحرج، وتعد جريمة الانتقام الاباحي من الجرائم التي تتم في البيئة الرقمية، التي عُلجت لدى العديد من التشريعات لكن مع ظهور تقنية التزييف العميق بات باستطاعة الشخص استخدام صور الأشخاص المنشورة والمتوفرة عبر المواقع الالكترونية لتظهر بصورة منافية للحياء ثم استخدامها للانتقام من الأفراد (علاء الدين منصور مغايرة، ٢٠٢٤، ١٣٧).ان الفيديوهات والتسجيلات المزيفة بتقنية التزييف العميق قد تؤدي أي زعزعة الاستقرار الأمني للمجتمع، وذلك عن طريق اختلاق مشاهد تتضمن اعتداء الشرطة على المواطنين، مما قد يؤدي الى التأثير على الرأي العام، والقيام بأعمال الشغب والتحريض على استعمال العنف، او انشاء فيديوهات تتضمن التصريحات المسيئة للسياسيين او القادة، والتي قد تؤدي الى نشوب التظاهرات والشعب والتعدي على الأموال والمصالح العامة (رباب مصطفى عبد المنعم الحكيم، ٢٠٢٥، ٢٦٩٠)مما ذكر أعلاه تُعدّ جريمة الذكاء الاصطناعي في هذا النوع من الجرائم من أخطر التطبيقات غير المشروعة لتقنية التزييف العميق (Deepfake)، وهي استخدامها كأداة لإثارة الفتنة وزعزعة استقرار المجتمعات، من خلال فبركة مشاهد تُظهر اعتداءات غير حقيقة من أجهزة الشرطة بحق الاشخاص، أو من خلال التلاعب بخطابات السياسيين او القادة او المسؤولين، وهو ما يمثل تهديدًا مباشرًا للأمن القومي والسلم الاجتماعي، فمثل هذه الفيديوهات، وإن كانت مزيفة، إلا أنها تتمتع بدرجة عالية من الإقناع البصري والسمعي، مما يُمكّنها من التأثير في الرأي العام بصورة كبيرة، خصوصًا في بيئات مشحونة أو تعاني من انقسام سياسي أو اجتماعي، وقد تُستغل في حملات تضليل ممنهجة أو تدخلات أجنبية في الشؤون الداخلية للدول.ومن الزاوية القانونية، فإن هذا النمط من الأفعال يتقاطع مع عدة صور من التجريم، منها الأفعال التحريضية على العنف، ونشر أخبار كاذبة، ومساس الأمن العام، فضلًا عن انتهاك الخصوصية وسُمعة الأشخاص، ما يفرض على المشرّعين ضرورة التدخل بتنظيم دقيق لوضع الاطار الخاص بتجريم استخدام تقنيات التزييف العميق في هذه السياقات، سواء عبر قوانين الإعلام أو مكافحة الجرائم المعلوماتية أو قوانين الأمن الوطني، مع ضرورة أن تكون النصوص القانونية مرنة وقابلة للتحديث لمواكبة التطور السريع لهذه التقنية.وعمليًا، فإن مواجهة هذا التهديد لا تقتصر على الجانب التشريعي فقط، بل تتطلب أيضًا تطوير أدوات تقنية قادرة على كشف التزييف، ورفع الوعي المجتمعي بمخاطر المحتوى الرقمي المفبرك، وتعزيز ثقافة التحقق من المعلومات، لا سيما في ظل الانتشار الواسع لمواقع التواصل التي تُعد حاضنًا رئيسيًا لانتشار هذه الفيديوهات دون رقابة فعالة.

المطلب الثاني الانتهاكات الناجمة عن التزييف العميق

رافق ظهور الحاسوب خطورة على الحياة الخاصة للأفراد، تمثلت في تهديد هذه الأدوات لحقوق الانسان، إذ باتت حياته عارية من الحماية أمام هذه الأجهزة، الأمر الذي ظهرت منه تساؤلات قانونية عديدة، منها هل إن نصوص قانون العقوبات والقوانين التقليدية الأخرى كافية لحماية الحياة الخاصة للأفراد؟ وسرية البيانات الشخصية؟ أم من الضروري وضع إطار قانوني جديد يساير حجم المخاطر ومواجهة هذه التحديات؟ من البين إن الاستغلال التجاري يمثل تحديًا خطرًا على البيانات الشخصية، والذي يتعمد في المقام الأول على تراكم المعلومات الرسمية والأساسية والتقنية المتعلقة بهوية الشخص، نظرًا لإن الاقتصاد الرقمي يعمد لحد ما على الإعلانات المستهدفة والتي تشارك فيها جهات فاعلة مختلفة (إبراهيم عطية محمود المهدي، ٢٠٢٣، ٥١٦) إن التشهير هو الاستخدام الأكثر لتقنية التزييف العميق لا سيما استخدامه في قذف الغير، عبر إنشاء ما يسمى

(أفلام اباحية مفبركة)، ولذا ظهرت حالات متعددة لابتزاز جنسي لفتيات عبر تقنية التزييف العميق، وتشير إحدى التقارير إن غالبية البيانات الملفقة عبر هذه التقنية تكون في المواد الإباحية، ولذا أكد الخبراء ان هذه التقنية إذ استخدمت مع أدوات إخفاء الهوية، فإنها تلحق ضررًا بالغاً (احمد مصطفى معوض محمد محرم، ٢٠٢٢، ٢٥٣٦)من المعلوم بان علة التجريم لاي منهج عقابي هو المحافظة على المصلحة الجوهرية في المجتمع، فالقانون حين يجرم السرقة يكون لعلة الاعتراف بحق الملكية كقيمة من قيم المجتمع، وعندما يجرم القتل فذلك أيضًا لاعترافه بالحق في الحياة كقيمة يسعى المجتمع لحمايتها، والامر ذاته عندما يتدخل لتجريم أفعال الاعتداء على حرمة الحياة الخاصة، فهي تختص بالحماية الدستورية بصفة عامة وبالحماية الجزائية بصفة خاصة (بارق منتظر عبد الوهاب لامي، ٢٠١٧، ٩٤)لذا نجد ان المشرع في مصر سار وفقًا لهذا المبدأ من أجل الحماية الخاصة بالأفراد، إذ أشار صراحة بانه كل شخص اعتدى بأي صورة على مبادئ أو قيم الأُسرة المصرية أو انتهك الحرمة الخاصة بالحياة الخاصة للأفراد، أو عمل على ارسل العديد من الرسائل الإلكترونية بكثافة لشخص معين دون الحصول على موافقته، أو القيام بنشر معلومات عن طريق شبكة الإنترنت أو بإحدى وسائل تقنية المعلومات أو اخبارًا أو صورًا وما في حكمها، تنتهك الخصوصية لأي شخص دون رضاه، سواء كانت المعلومات المنشورة دقيقة او غير دقيقة بعقوبة الحبس مدة لا تقل عن ستة اشهر، وبغرامة أو تكون إحدى العقوبتين المشار اليها (الجريدة الرسمية– العدد ٣٢ مكرر (ج) في ١٤ أغسطس سنة ٢٠١٨.)من هذا النص يتبين لنا إن القانون المصري قد أشار صراحة إلى إن انتهاك حرمة الحياة الخاصة من خلال نشر الصور أو الأخبار بإي صورة كانت صحيحة أو مزيفة، وبهذا فقد تصدى المشرع لهذه الأفعال الخطرة بحزم، كما ويُعد النص الوارد في القانون رقم ١٧٥ لسنة ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات تعبيرًا عن توجه تشريعي متقدم يهدف إلى تعزيز الحماية الجنائية للخصوصية الرقمية والحياة الخاصة في ظل تصاعد الانتهاكات الإلكترونية، إذ جرَّم المشرّع المصري أفعالًا متعددة من بينها الأفعال التي تهدد القيم الاسرية، او التي تنتهك انتهاك الحرمة الخاصة بالأفراد، والقيام بإرسال الرسائل الإلكترونية بكثافة دون رضا المتلقي، أو نشر معلومات أو صور دون موافقة صاحبها، سواء كانت صحيحة أو غير صحيحة، ما يُظهر فهمًا عميقًا لطبيعة الخصوصية بوصفها قائمة على الإرادة وليس فقط على صحة المحتوى، إلا أن النص يشوبه بعض الغموض التشريعي، خصوصًا في استخدامه لعبارات فضفاضة (كالقيم الأسرية) و (الكثافة في الإرسال)، دون تحديد ضوابط واضحة، مما قد يفتح الباب أمام الاجتهادات القضائية العديدة ويُهدد بصورة أساس مبدأ مهم من المبادئ التي يقوم عليها القانون الجنائي ألا وهو شرعية الجريمة والعقوبة، كما أن وضع نشر المعلومات الصحيحة في اطار التجريم دون مراعاة لوجود مصلحة عامة قد يمس بحرية التعبير، وعليه فإن النص يتطلب إيضاحات تفسيرية أو تعديل تشريعي يحقق التوازن بين حماية الخصوصية وضمان الحقوق الدستورية في التعبير، مع دعم القضاة المتخصصين في هذا النوع من الجرائم بالتدريب المستمر لضمان حسن التطبيق.وحين التطرق لما جاء في القانون في دولة الامارات بانه قد أشار صراحة بعقوبة الحبس مدة لا تقل عن (٦) ستة أشهر والغرامة، أو إيقاع احدى العقوبتين على كل شخص استخدم الشبكة المعلوماتية، أو النظام المعلوماتي الإلكتروني، أو إحدى الوسائل التقنية، قاصدًا منها إيقاع الاعتداء على الخصوصية المتعلقة بالأشخاص أو على حرمة الحياة الخاصة أو العائلية لهم من غير توافر عنصر الرضا وفي غير ما نص عليه القانون وكما ذكرت وفقًا للطرق الآتية:

1 – استراق السمع، أو اعتراض، أو تسجيل أو نقل أو بث أو إفشاء محادثات أو اتصالات أو مواد صوتية أو مرئية.

2 – التقاط صور الغير في أي مكان عام أو خاص أو إعداد صور إلكترونية أو نقلها أو كشفها أو نسخها أو الاحتفاظ بها.

3 – نشر أخبار أو صور إلكترونية أو صور فوتوغرافية أو مشاهد أو تعليقات أو بيانات أو معلومات ولو كانت صحيحة وحقيقية بقصد الإضرار بالشخص.

4 – التقاط صور المصابين أو الموتى أو ضحايا الحوادث أو الكوارث ونقلها أو نشرها بدون تصريح أو موافقة ذوي الشأن.

5 – تتبع أو رصد بيانات المواقع الجغرافية للغير أو إفشاءها أو نقلها أو كشفها أو نسخها أو الاحتفاظ بها.

كما انه أشار القانون لعقوبة الحبس مدة لا تقل عن سنة أو إيقاع إحدى العقوبتين المشار اليها، كل شخص استخدم النظام المعلوماتي الإلكتروني، أو إحدى الوسائل التقنية، من أجل إجراء تعديل أو معالجة على تسجيل أو صورة أو مشهد، قاصدًا منها التشهير أو الإساءة للأشخاص.من خلال ذلك يعكس التشريع الإماراتي نهجًا صارمًا ومتقدمًا في حماية الخصوصية الرقمية وحرمة الحياة الخاصة، حيث نص على عقوبات مشددة لأي مستخدم للشبكات أو أنظمة المعلومات أو عبر الوسائل المعلوماتية بهدف الاعتداء على خصوصية الأفراد دون رضاهم وبالمخالفة للقانون، سواء تم ذلك عبر استراق السمع أو تسجيل أو بث المحادثات أو الصور أو الفيديوهات، أو من خلال نشر مواد – حتى وإن كانت صحيحة – بقصد الإضرار، إضافة إلى تجريم تتبع المواقع الجغرافية أو نشر صور المصابين أو الموتى دون موافقة ذوي الشأن، وهو ما يشير إلى توسّع في صور

السلوك الإجرامي بما يغطي مظاهر الاعتداء المعلوماتي الأكثر شيوعًا في العصر الرقمي.كما شدد المشرع العقوبة لتصل إلى الحبس والغرامة في حال استخدام تقنيات المعلومات لتعديل الصور أو المشاهد بقصد التشهير أو الإساءة، وهو ما يؤكد حرص المشرع الإماراتي على مواجهة ظواهر مثل التزوير الرقمي (Deepfake) أو التشويه البصري للسمعة. ويُلاحظ أن القانون اعتمد على معايير دقيقة ومفصلة لتحديد الأفعال المُجرّمة، ما يحقق الوضوح واليقين القانوني، ويُسهم في منع إساءة استخدام الفضاء الرقمي بما يمس بكرامة الأفراد وحياتهم الخاصة.ومن خلال ما تم البحث عنه ودراسته فان التزييف العميق (Deepfake) يمثل أحد أخطر تطبيقات الذكاء الاصطناعي في العصر الرقمي، حيث تزايدت استخداماته في إنتاج محتوى مرئي وصوتي يصعب تمييزه عن الحقيقي، وأظهر هذا النوع من التقنية تهديدًا متعدد الأبعاد، شمل النواحي الأمنية عبر تهديد الاستقرار السياسي والتأثير على الرأي العام، وخلق بيئة خصبة لنشر المعلومات المضللة، فضلًا عن مخاطر التجسس والابتزاز الإلكتروني سواء استهدف الأشخاص او المؤسسات.أما من الجانب القانونية، فقد كشفت تقنيات الذكاء الاصطناعي عن قصور في التشريعات لدى العديد من النظم القانونية من بينها العراق الذي يعد من بين الدول التي لم تواكب تشريعاتها التطور التقني، ما أدى إلى تحديات جدية في إثبات الجرائم والتصدي لها، وتحديد المسؤولية الجنائية، وحماية الحقوق الفردية مثل السمعة والخصوصية.ومن ثمّ، فإن مواجهة هذه التهديدات تقتضي تطوير الأطر القانونية القائمة، ووضع معايير تقنية لكشف المحتوى المزيف، إلى جانب تعزيز الوعي المجتمعي بخطورة هذه الممارسات، لتحقيق التوازن بين الابتكار الرقمي والحماية القانونية الفعالة.

الخاتمة

أظهر التزييف العميق باعتباره أحد مخرجات الذكاء الاصطناعي التوليدي، أنه لا يقتصر على التلاعب بالمحتوى الرقمي فحسب، بل يمتد إلى تهديد أسس الثقة في المعلومات، وتقويض الأمن الرقمي، وإحداث ارتباك قانوني في تصنيف وتكييف الأفعال الناجمة عنه.إن استمرار الاعتماد على الأطر القانونية التقليدية لم يعد كافيًا لمواجهة هذا النمط الجديد من الجرائم، لا سيما في ظل ضعف القدرة على اكتشاف التزييف، وصعوبة إثبات النية الإجرامية، وتحديد المسؤولية الجنائية في البيئة الافتراضية والتي لا تهتم بالحدود، ومن ثم، فإن تحقيق التوازن بين حماية الحقوق والحريات الرقمية من جهة، وضمان الأمن العام ومنع إساءة استخدام التكنولوجيا من جهة أخرى، يفرض على المشرع والقاضي والباحث القانوني مسؤولية مشتركة لإعادة صياغة المفاهيم القانونية بما يتلاءم مع واقع الجريمة الرقمية المعاصرة.ومن خلال التحليل الذي قدمه هذا البحث، يتضح أن مجابهة التزييف العميق تتطلب استراتيجية متعددة الأبعاد تشمل: تطوير التشريعات، دعم الأجهزة الأمنية والقضائية فنيًا، وتوعية المجتمع بخطورة هذه الظاهرة. وبدون هذه الركائز، ستبقى البيئة الرقمية عرضة لتصاعد الجرائم ذات الطابع التكنولوجي، بما فيها التزييف العميق، بما يشكل تهديدًا مستمرًا للثقة العامة والنظام القانوني.

أولاً: النتائج

– يمثل التزييف العميق جريمة رقمية مركبة تتداخل فيها عدة صور من السلوك غير المشروع، مثل التزوير، والاحتيال، وانتهاك الخصوصية، والتحريض، مما يصعّب تصنيفها ضمن إطار قانوني تقليدي واحد.

– تُظهر التشريعات الجنائية التقليدية –ومنها القانون العراقي– قصورًا في معالجة التزييف العميق بصفته ظاهرة رقمية متطورة، لا سيما من ناحية التجريم المباشر، وتعريف الأركان المادية والمعنوية للجريمة، وأدوات الإثبات الرقمية.

– يُستغل التزييف العميق في حملات تضليل إعلامي، وزعزعة الثقة بالمؤسسات العامة، وتشويه سمعة الشخصيات السياسية والاجتماعية، مما يجعله تهديدًا مباشرًا للأمن القومي والسلم المجتمعي.

– يفرض التزييف العميق تحديات خطيرة أمام سلطات التحقيق والقضاء، إذ يصعب التمييز بين المقاطع الأصلية والمزيفة، مما قد يؤدي إلى تضليل العدالة أو إنكارها.

– ما يزال الوعي العام بمخاطر التزييف العميق منخفضًا، سواء لدى الأفراد أو المؤسسات، مما يزيد من فرص الوقوع ضحية أو استخدام هذه التقنية دون إدراك لطبيعتها الجرمية.

ثانياً: التوصيات

– من المهم بل الضروري إدراج جرائم التزييف العميق في قانون العقوبات أو إصدار تشريع خاص بمكافحة جرائم تقنية المعلومات يتضمن تعريفًا دقيقًا لهذا النوع من الجرائم، وأركانًا قانونية واضحة، مع عقوبات تتناسب مع جسامة الأثر.

– تعزيز قدرات المحققين والقضاة في مجال الأدلة الرقمية، والتعرف على التقنيات المستخدمة في التزييف العميق، من خلال برامج تدريب متخصصة بالتعاون مع خبراء تكنولوجيا المعلومات.

– الاستثمار في التكنولوجيا المساعدة لكشف التزييف العميق من بينها البرامج الخاصة بتحليل البيانات البيومترية والصوتية، وتمكين الجهات المختصة سواء التي تقوم بالتحقيق اصالة او استثناءً من استخدامها في التحقيقات الجنائية.

– نظرًا للطبيعة العابرة للحدود لهذه الجرائم، يوصى بتعزيز التعاون مع المنظمات الدولية والدول الأخرى لتبادل الخبرات، والمساعدة القانونية، وتعقب الجناة عبر الحدود.

– تنفيذ حملات توعوية حول خطورة استخدام أو تداول محتوى التزييف العميق، وبيان التصورات المتعقلة بالمخالفة للقانون المترتبة عليه، سواء من ناحية الأفراد أو المنصات الإعلامية.

– دعم تشكيل وحدات أمنية وقضائية متخصصة في الجرائم الرقمية، مع تركيز جزء منها على جرائم التزييف العميق، لتسريع الاستجابة والحد من الأضرار.

المصادر

القوانين:

– قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ وتعديلاته.

– قانون رقم ١٧٥ لسنة ٢٠١٨ في شأن مكافحة جرائم تقنية المعلومات، الجريدة الرسمية، العدد ٣٢ مكرر (ج) في ١٤ أغسطس ٢٠١٨، مصر.

الكتب:

– دليل التزييف العميق، الامارات، ٢٠٢١.

الرسائل والاطاريح:

– ريم غريب علي حمدان الشامسي، حماية الخصوصية في ظل تطبيقات الذكاء الاصطناعي (دراسة تحليلية مقارنة)، رسالة ماجستير، كلية القانون، جامعة الامارات العربية المتحدة، الامارات، ٢٠٢٢.

– حسين عباس حميد، المسؤولية الجنائية عن الاستخدام غير المشروع للذكاء الاصطناعي دراسة مقارنة، أطروحة دكتوراه، كلية الحقوق، جامعة الإسكندرية، مصر، ٢٠٢٤.

– بارق منتظر عبد الوهاب لامي، جريمة انتهاك الخصوصية عبر الوسائل الالكترونية في التشريع الأردني، رسالة ماجستير، جامعة الشرق الأوسط، كلية الحقوق، الأردن، ٢٠١٧.

الأبحاث العلمية:

– سامح محمد محمد السيد إبراهيم، المخاطر الأمنية والمجتمعية للتزييف العميق وآليات المواجهة، المجلة القانونية، المجلد ٢٣، العدد ٧، كلية الحقوق– فرع الخرطوم، جامعة القاهرة، ٢٠٢٥، ص ٣٩٦٦.

– بن عودة حسكر مراد، إشكالية تطبيق احكام المسؤولية الجنائية عن جرائم الذكاء الاصطناعي، مجلة الحقوق والعلوم الإنسانية، المجلد ١٥، العدد ١، جامعة زيان عشور الجلفة، الجزائر، ٢٠٢٢، ص ١٩٧.

– محمد عباس حمودي حسين الزبيدي ونور قيس محمد شاهين، أزمة النص الجنائي في مواجهة جرائم الذكاء الاصطناعي، دراسة تحليلية، مجلة جامعة الزيتونة الأردنية للدراسات القانونية، العدد خاص، جامعة الزيتونة، الأردن، ٢٠٢٤، ص ٢٩.

– احمد عبد الموجود أبو الحمد زكير، جريمة التزييف الاباحي العميق، المجلة القانونية، المجلد ١١، العدد ٧، ، ، ٢٠٢٢، ص ٢٢٨٠.

– الذكاء الاصطناعي ومخاطر التزييف العميق، مجلس الوزراء –مركز المعلومات ودعم اتخاذ القرار، مصر، ٢٠٢٣.

– سامح محمد محمد السيد االبراهيم، المخاطر الأمنية والمجتمعية للتزييف العميق وآليات المواجهة، ٢٣، العدد ٧، ٢٠٢٥، ص ٣٩٧٤.

– علاء الدين منصور مغايرة، جرائم الذكاء الاصطناعي وسبل مواجهتها: جرائم التزييف العميق انموذجًا، المجلة الدولية للقانون، المجلد الثالث عشر، العدد المنتظم الثاني، جامعة قطر، كلية القانون، قطر، ٢٠٢٤، ص ١٣٧.

– رباب مصطفى عبد المنعم الحكيم، الجوانب القانونية للتزييف العميق، مجلة البحوث الفقهية والقانونية، العدد ٤٨، مجلة الازهر، كلية الشريعة والقانون بدمنهور، مصر، ٢٠٢٥، ص ٢٦٩٠.

– إبراهيم عطية محمود المهدي، الحق في الهوية الرقمية في ضوء حماية البيانات الشخصية والخصوصية المعلوماتية، مجلة البحوث القانونية والاقتصادية، العدد ٨٤، جامعة المنصورة، كلية الحقوق، مصر، ٢٠٢٣، ص ٥١٦.

– احمد مصطفى معوض محمد محرم، استخدامات الذكاء الاصطناعي استخدام تقنية التزييف العميق في قذف الغير نموذجًا، مجلة البحوث الفقيه والقانونية، المجلد ٣٤، العدد ٣٩، جامعة الازهر،

المصادر الأجنبية:

− S.B. No. 751, AN ACT, relating to the creation of a criminal offense for fabricating a deceptive video with intent to influence the outcome of an election, https://capitol.texas.gov/tlodocs/86R/billtext/html/SB00751F.htm.

− Cal. Elec. Code § 20010 ،https://www.dwt.com/blogs/media-law-monitor/2020/02/two-new-california-laws-tackle-deepfake-videos-in

References

• Legislation:

•Iraqi Penal Code No. 111 of 1969, as amended.

•Law No. 175 of 2018 on Combating Information Technology Crimes, Official Gazette, Issue No. 32 (bis C), August 14, 2018, Egypt.

• Books:

•*Deepfake Guide*, United Arab Emirates, 2021.

• Theses and Dissertations:

•Reem Gharib Ali Hamdan Al Shamsi, *Protection of Privacy in Light of Artificial Intelligence Applications: A Comparative Analytical Study*, Master's Thesis, College of Law, United Arab Emirates University, UAE, 2022.

•Hussein Abbas Hameed, *Criminal Liability for the Unlawful Use of Artificial Intelligence: A Comparative Study*, PhD Dissertation, Faculty of Law, Alexandria University, Egypt, 2024.

•Barq Montathar Abdulwahab Lami, *The Crime of Privacy Violation through Electronic Means in Jordanian Legislation*, Master's Thesis, Middle East University, Faculty of Law, Jordan, 2017.

• Scholarly Articles:

•Sameh Mohamed Mohamed El-Sayed Ibrahim, *Security and Societal Risks of Deepfake and Mechanisms of Confrontation*, Al-Qanoun Journal, Vol. 23, Issue 7, Faculty of Law – Khartoum Branch, Cairo University, 2025, p. 3966.

•Ben Aouda Haskar Mourad, *The Problem of Applying Criminal Responsibility to AI Crimes*, Journal of Law and Human Sciences, Vol. 15, Issue 1, Ziane Achour University of Djelfa, Algeria, 2022, p. 197.

•Mohammed Abbas Hammoudi Hussein Al-Zubaidi & Nour Qais Mohammed Shaheen, *The Crisis of Legal Texts in Confronting AI Crimes: An Analytical Study*, Journal of Legal Studies, Special Issue, Al-Zaytoonah University of Jordan, 2024, p. 29.

•Ahmed Abdel-Mawgoud Abu El-Hamd Zakir, *The Crime of Deepfake Pornography*, Al-Qanoun Journal, Vol. 11, Issue 7, Faculty of Law – Khartoum Branch, Cairo University, Egypt, 2022, p. 2280.

•*Artificial Intelligence and Deepfake Risks*, Cabinet of Ministers – Information and Decision Support Center (IDSC), Egypt, 2023.

•Sameh Mohamed Mohamed El-Sayed Ibrahim, *Security and Societal Risks of Deepfake and Mechanisms of Confrontation*, Al-Qanoun Journal, Vol. 23, Issue 7, Faculty of Law – Khartoum Branch, Cairo University, Egypt, 2025, p. 3974.

•Alaa Al-Din Mansour Mughayrah, *Artificial Intelligence Crimes and Methods of Confrontation: Deepfake Crimes as a Model*, International Journal of Law, Vol. 13, Regular Issue 2, Qatar University, Faculty of Law, Qatar, 2024, p. 137.

•Rabab Mostafa Abdel Moneim Al-Hakim, *Legal Aspects of Deepfake*, Journal of Jurisprudence and Legal Research, Issue 48, Al-Azhar University, Faculty of Sharia and Law – Damanhur, Egypt, 2025, p. 2690.

•Ibrahim Atiyah Mahmoud Al-Mahdi, *The Right to Digital Identity in Light of Personal Data Protection and Information Privacy*, Journal of Legal and Economic Research, Issue 84, Mansoura University, Faculty of Law, Egypt, 2023, p. 516.

•Ahmed Mostafa Moawad Mohammed Moharram, *Uses of Artificial Intelligence: Deepfake Technology as a Tool for Defamation*, Journal of Jurisprudence and Legal Research, Vol. 34, Issue 39, Al-Azhar University, Faculty of Sharia and Law, Egypt, 2022, p. 2536.

• Foreign Sources:

•S.B. No. 751, *An Act relating to the creation of a criminal offense for fabricating a deceptive video with intent to influence the outcome of an election*, Texas Legislature, Link.

•Cal. Elec. Code § 20010, *Two New California Laws Tackle Deepfake Videos in Politics*, Link.