التكييف القانوني لجريمة التزييف العميق

(دراسة مقارنة)

The Legal Adaptation of Violent Forgery (Comparative Study)

صابرين جاسم مكطوف

أ.م.د. اميل جبار عاشور

Sabreen Jaslm Makttoof

Dr.Ameel Jabbar Ashour

ameelashour@uomisan.edu.iq

07706065831

جامعة ميسان / كلية القانون

تاريخ استلام البحث

٢٠٢٥/٣/٨

تاريخ قبول البحث

٢٠٢٥/٤/٨

المستخلص

تعد جريمة التزييف العميق من الجرائم الرقمية التي تقع باستخدام تقنيات الذكاء الاصطناعي من خلال استخدام شبكة الخصومة التوليدية التي تعمل على توليد وانتاج محتوى مرئي كان أو صوتي مشابهة للحقيقية والواقع ولا يمكن تميزه ومعرفته من قبل عامة الناس، لما يتمتع هذا المحتوى المزيف من دقة واحترافية عالية، وان الغرض من انشاء هذا المحتوى المزيف قد يكون لأغراض تشهير وابتزاز الضحية من اجل غاية او هدف يسعى اليها الجاني، كما ان هذه الجريمة ترتكب من اجل القيام بارتكاب جرائم الاحتيال المالي التي تقع على المؤسسات العامة والخاصة، اذ تكمن اهمية البحث كون جريمة التزييف العميق من الجرائم الحديثة العابرة للحدود الجغرافية للدول، ولما لها من مخاطر واضرار تمس الدول والمجتمعات، الا انه وجدنا غياب التشريعات محل الدراسة عن ذكر نصوص قانونية واضحة وصريحة تجرمها، مما يتوجب الرجوع الى القوانين العقابية العامة والخاصة بمكافحة الجرائم المعلوماتية من اجل معالجة وسد النقص التشريعي الموجود فيها، من خلال ايجاد التكييف القانوني المناسب لجريمة التزييف العميق، لكي يمكن مواجهتها ومنع افلات الجناة من العقاب. وعليه بينا هذا الموضوع من خلال تقسيم خطة البحث الى مبحثين، اذ بينا في المبحث الاول ماهية جريمة التزييف، وفي المبحث الثاني بينا التكييف القانوني لجريمة التزييف العميق في التشريع العراقي والدول محل المقارنة، لبيان مواطن القوى والضعف ومدى قدرة هذه القوانين في مواجهة جريمة التزييف العميق والسيطرة عليها، اذ نرى على الرغم من قدرة هذه القوانين لعقاب الجناة ومواجهة الجريمة، الا انه يجب ان يكون هناك نص قانوني صريح يجرمها ويعاقب عليها بعقوبة تلاءم شدتها وخطورتها.

الكلمات المفتاحية:(الذكاء الاصطناعي، التزييف العميق، التكييف القانوني، دوافع الجريمة).

Abstract

Deep fake crime is a digital offense that relies on artificial intelligence technologies, particularly Generative Adversarial Networks (GANs), to create and produce visual or audio content that closely resembles reality. This synthetic content is often indistinguishable from authentic material to the general public due to its high level of accuracy and sophistication. The primary purpose behind generating such manipulated content may involve defamation, blackmail, or extortion, serving the perpetrator’s specific objectives. Additionally, deepfake technology is frequently exploited to commit financial fraud against public and

private institutions. The significance of this study lies in the fact that deepfake crime is a modern transnational offense that poses severe risks and harms to nations and societies. However, our research has revealed the absence of explicit legal provisions that directly criminalize deepfake activities in the legislation under review. Consequently, it becomes necessary to refer to general and specialized laws on cybercrime to address and fill this legislative gap by establishing an appropriate legal classification for deepfake crime. This approach is essential to ensure that such offenses are effectively addressed and that perpetrators do not evade punishment. While existing laws provide mechanisms for prosecuting offenders, it is crucial to introduce explicit legal provisions that explicitly criminalize deepfake offenses and impose penalties that correspond to their severity and dangerous implications.

المقدمة

اولاً: مقدمة البحث:

لقد صاحب العالم اليوم في ظل تقدم وتطور العالم الرقمي، في مجال الذكاء الاصطناعي الى ظهور العديد من الجرائم التي تقع من خلال اساءه استخدام تقنيات الذكاء الاصطناعي، كما هو الحال في تقنية التزييف العميق(Deep Fake)، التي تعمل على انشاء محتوى مرئي أو صوتي سواء كانت تسجيلات صوتية أو مقاطع فيديو أو صور مزيفة تبدو وكأنها واقعية للغاية، مما تم اساءه استخدام هذه التقنية بطرق غير مشروعة من قبل المجرمين المعلوماتيين من أجل المساس بالحقوق المحمية بموجب القوانين، مما اثارت هذه التقنية العديد من المخاوف الاخلاقية والقانونية في المجتمعات والدول.

ثانياً: أهمية البحث:

تتجلى اهمية البحث في التكييف القانوني لجريمة التزييف العميق، لكون هذه الجريمة من الجرائم التي لم يوضع لها تشريع قانوني او نص قانوني خاص واضح ومباشر في التشريعات العربية، الا انه لما لهذه الجريمة من مخاطر واضرار ولاعتبارات قانونية واجتماعية وتقنية يمكن مواجهة هذه الجريمة من خلال الاعتماد على القوانين العقابية التقليدية العامة والخاصة، من أجل البحث عن تكييف قانوني مناسب لنشاط النشاط الجرمي من اجل سد الفراغ التشريعي في القوانين العقابية وحماية لحقوق وحريات الافراد الشخصية.

ثالثاً: مشكلة البحث:

تتمثل اشكالية البحث في ان جريمة التزييف العميق من الجرائم التي تعمل على انشاء صور وفيديوهات مزيفة تبدو وكأنها حقيقة بالاعتماد على التعلم الالي والتعلم العميق ونشرها على مواقع التواصل، من أجل انتهاك خصوصية الافراد والتشهير بهم وابتزازهم، وتبرز اشكالية البحث الاساسية في البحث عن التكييف القانوني لجريمة التزييف العميق في ظل غياب النصوص القانونية الصريحة في التشريع العراقي والدول محل المقارنة، ومدى ملائمة القوانين العقابية الحالية لمواجهتها.

رابعاً: منهجية البحث ونطاقة:

انسجاماً مع طبيعة هذا البحث سوف يتم اعتماد المنهج التحليلي والمقارن أساساً له، من خلال المنهج التحليلي يمكننا تحليل النصوص القانونية ذات الصلة، وكذلك تحليل الاحكام والقرارات القضائية، اما في المنهج المقارن الذي يمكن من خلاله العمل على مقارنة بين النصوص القانونية في العراق والتشريعات محل المقارنة من أجل التعرف على مواطن القصور والقوة في القوانين العقابية الخاصة بمكافحة الجرائم المعلوماتية في الامارات ومصر وفي قانون العقوبات العراقي رقم (١١) لسنة ١٩٦٩ المعدل.

خامساً: خطة البحث:

من أجل بيان موضوع البحث من كافة جوانبه، سوف نقسم البحث على مبحثين: في المبحث الاول سوف نبين ماهية جريمة التزييف العميق، وفي المبحث الثاني سوف نبين التكييف القانوني لجريمة التزييف العميق واثارها.

المبحث الاول

ماهية جريمة التزييف العميق

في السابق كان برنامج الفوتوشوب من أحد وأشهر التطبيقات المعروفة والمستخدمة في دمج وتركيب الصور المفبركة، لكن مع تطور التكنولوجيا والذكاء الاصطناعي ظهرت تقنية التزييف العميق التي تعمل على انشاء وانتاج محتوى مرئي أو صوتي مزيف للأشخاص تبدو وكأنها واقعية، حيث ان لهذه التقنيات العديد من الايجابيات ومنها في مجال التعليم والصحة والثقافة والفن كإنتاج المسلسلات والافلام، الا أنه تم اساءه استخدامها من قبل الجناة لأغراض خبيثة واحتيالية من اجل ارتكاب جرائم التشهير والابتزاز

والاحتيال المالي وغيرها من الصور الجرمية التي تقع خلال استخدام هذه التقنية[١]. وعليه سوف نبين تعريف جريمة التزييف العميق وخصائصها في المطلب الاول، وفي المطلب الثاني سوف نبين انواع التزييف العميق وآثاره.

المطلب الاول

تعريف جريمة التزييف العميق وخصائصها

تعد جريمة التزييف العميق من الجرائم المرتكبة باستخدام الحاسب الالي وشبكة الانترنت، ويعتمد ارتكاب هذه الجريمة من خلال الاعتماد على التعلم الالي والتعلم العميق من اجل توليد محتوى مزيف والذي شمل الصور والفيديوهات والتسجيلات الصوتية، مما اثارت هذه التقنية العديد من المخاطر الأخلاقية، وعلية سوف نتطرق الى تعريف جريمة التزييف العميق وخصائصها[٢].

الفرع الاول

تعريف جريمة التزييف العميق

تعد جريمة التزييف العميق من الجرائم المستحدثة التي ظهرت مع ظهور وتطور الذكاء الاصطناعي، لذا سوف نتطرق الى تعريفها من خلال بيان التعريف اللغوي والاصطلاحي والفقهي لها.

اولاً: تعريف التزييف العميق لغة.

ان معنى التزييف في اللغة العربية معناه الرداءة والغش، وهي مشتقة من كلمة زافَ، يَزفُ، زِيْفاً وزَيفاناً[٣]، ومصدر (زيّف) من زاف الدرهم يَزيف زُيوفًا، اي رَديئةً، (وزُيوفَة) فهو زائف، والجمع (زُيفُ)، وزيَّفَ الرجل: صغر به وحقَّره، مأخوذ من الدرهم الزائف، وهو الرديء[٤].

(١) د. محمود زكي زيدان، المواجهة الجنائية للاستخدام غير المشروع لتقنية التزييف العميق(دراسة مقارنة)، ط١، دار الفكر والقانون للنشر والتوزيع، مصر، ٢٠٢٥، ص١٧.

(٢) د. أشرف سيد أبو العلا، المواجهة الجنائية لمخاطر تقنية الديب فيك (Deep fake) واثرها على حجية الادلة الرقمية في الاثبات الجنائي (دراسة تحليلية مقارنة)، ط ١، دار النهضة العربية، مصر، ٢٠٢٤، ص ١٥.

(٣) ابو الفضل جمال الدين محمد بن مكرم بن منظور، لسان العرب، ج ٩، ط ١، دار صادر، بيروت، ١٩٩٨، ص ١٤٣.

(٤) أبو الحسن علي بن اسماعيل والمعروف بأبن سيده، المحكم والمحيط الاعظم، ج ١١، ط ١، دار الكتب العلمية، بيروت، ٢٠٠٠، ص ٩٣.

المعنى اللغوي لمفردة العميق: فهو صفة مشبهَّة تدلّ على الثبوت من (عمُقَ)، وعَمَّقَ النَّظَرَ في مَوْضُوعِهِ: أَطَالَ فيهِ النَّظَرَ بِرَوِيَّةٍ،(وعَمِيق) طويل بعيد المسافة، ويقال: تحليل عميق للموقف: تحليل دالّ على وعي وذكاء وفِطنة، (وعَمُقَتِ) بَلغَتْ أَقْصَى كُنْهِهَا، وتَحَدَّثَ بعُمْقٍ في المَوْضُوعِ بِتَفْكِيرٍ وَرَوِيَّةٍ[١].

ثانياً: التعريف الاصطلاحي للتزييف العميق.

من اجل تعريف جريمة التزييف العميق من الناحية الاصطلاحية، فأنه يقتضي التطرق الى التعريف التشريعي والتعريف الفقهي، كما يلي :

١- التعريف التشريعي لجريمة التزييف العميق: لقد جاء مصطلح التزييف في جميع التشريعات مقترنا بالمسكوكات والعملات النقدية، كما ان اغلب التشريعات لم تضع او تتعرض الى بيان او مفردة التزييف في التشريعات الخاصة بالجرائم المعلوماتية وهذا ما زاد هذا الامر صعوبة على اعمال السلطة القضائية وهذا ما انتهت إليه المحاكم الامريكية[٢].

وعند الاطلاع على نصوص تشريعات الدول محل المقارنة مصر والامارات، والتشريعات العراقية لم نقف على تعريف للتزييف العميق، وإنما جاء مصطلح التزييف في قانون العقوبات المصري في المادة (٢٠٢/ فقرة الثانية) وعرف التزييف بأنه (يعتبر انتقاص شيء من معدن العملة أو طلاؤها بطلاء يجعلها شبيهة بعملة أخرى اكثر منها قيمة)[٣]، ومن خلال مطالعة نصوص المشرع المصري لم نرى تعريف للتزييف العميق، الا انه ربط مفهوم التزييف بالعملات المعدنية والورقية، وعلى الرغم من ان مصر شرعت قانون خاص في شأن مكافحة جرائم تقنية المعلومات رقم(١٧٥) لسنة ٢٠١٨، الا انها لم تعرف او تتعرض الى التزييف الذي يقع باستخدام الحاسب الالي وشبكات الانترنت[٤]. اما في الامارات العربية المتحدة ايضا ربطت مفهوم التزييف بالعملات والاوراق الورقية والمعدنية في قانون العقوبات الاماراتي في المادة (٢٠٤) ولم يعرفه او يشر اليه من باب الجرائم الالكترونية[٥]، كما جاء في قانون مكافحة الشائعات والجرائم

(١) أكرم كريم خضير، دراسات معمقة في فلسفة القانون الجنائي، المركز الاكاديمي للنشر، الاسكندرية، مصر، ٢٠٢٣، ص ١٢١- ١٢٢.

(٢) د. براء منذر كمال، د. مريفان مصطفى رشيد، دور القانون في حماية حقوق الإنسان من التزوير العميق، بحث شارك به في المؤتمر الدولي السنوي الخامس بعنوان (الاسلام حياة)، برعاية جامعة وارث الانبياء وبإسناد من بيت الحكمة والمجمع العلمي العراقي ومعهد العلمين للدراسات العليا، ٢٠٢٤، ص ١٠.

(٣) المادة (٢٠٢) من قانون العقوبات المصري رقم (٥٨) لسنة ١٩٣٧ المعدل.

(٤) قانون مكافحة جرائم تقنية المعلومات المصري رقم (١٧٥) لسنة ٢٠١٨.

(٥) المادة (٢٠٤) من قانون العقوبات الاماراتي رقم (٣) لسنة ١٩٨٧ المعدل.

الالكترونية رقم (٣٤) لسنة ٢٠٢١، خالي من كلمة التزييف فيما يتعلق بالجرائم الالكترونية[١]. كما ان المشرع العراقي في قانون العقوبات العراقي لم يعرف التزييف الا انه اشار الى كلمة التزييف في مواضع من النصوص القانونية المختلفة بخصوص التزييف الذي يقع على العملات المعدنية والورقية والطوابع والسندات المالية او المحررات الرسمية[٢]، كما انه العراق ما زال لم يشرع قانون خاص بمكافحة الجرائم الالكترونية، وان كل ما يوجد لدينا هو مشروع قانون مكافحة الجرائم الالكترونية لسنة ٢٠١٩، الا انه لا توجد فيه اي اشارة الى التزييف العميق بصورة خاصة او اي تنظيم قانوني للذكاء الاصطناعي وتقنياته بصورة عامة[٣].

٢- **التعريف الفقهي لجريمة التزييف العميق:** تعد جريمة التزييف العميق من نتائج التطور الذي شهدة عصر الذكاء الاصطناعي، حيث تعمل هذه التقنية على توليد محتوى مزيف سواء كان مرئي او صوتي من خلال استخدام مجموعة من الادوات والاساليب التي تتيح انتاج محتوى مزيف وغير حقيقي لأشخاص وهم يقولون أو يفعلون حركات لم يقوموا بها في الواقع من خلال استخدام التعلم الالي والتعلم العميق، لذا كان هناك العديد من التعريف بشأن جريمة التزييف العميق ومنها عرف بأنه "هو شكل من اشكال التلاعب البصري والصوتي الذي يتيح امكانيه توليد محاكاه واقعية لوجه شخص ما او صوته او حركاته، مما يبدو ان هذا الشخص قد فعل امراً او قال كلام وهو لم يقم به في الحقيقة"[٤]. وعرفها اخرون بأنها "طريقة من طرق التلاعب بالأصوات والصور ولفيديوهات باستخدام تقنيات وبرامج الذكاء الاصطناعي مع صعوبة اكتشافه من قبل عامة الجمهور لغرض تحقيق اهداف واغراض معينة"[٥]، كما عرف بأنه" احدى تطبيقات الذكاء الاصطناعي التي تعمل على تركيب محتوى الفيديوهات بشكل دقيق يحاكي الفيديو الاصلي وان كان يختلف عنه في مضمونه ومحتواه"[٦].

(١) قانون مكافحة الشائعات والجرائم الالكترونية الاماراتي رقم(٣٤) لسنة ٢٠٢١ المعدل.

(٢) المواد (٩، ٩٩، ٢٨٠، ٢٨٤) من قانون العقوبات العراقي رقم(١١١) لسنة ١٩٦٩ المعدل.

(٣) مشروع قانون مكافحة الجرائم الالكترونية العراقي لسنة ٢٠١٩.

(٤) حياة بلواضح، سماح بن ابراهيم، استخدام تقنية الذكاء الاصطناعي (التزييف العميق) في الفبركة الاعلامية – دراسة تحليله لعينة من الفيديوهات المنشورة على منصة تويتر الانتخابات الرئاسية الامريكية لسنة ٢٠٢٠ نموذجا، رسالة ماجستير، كلية العلوم الانسانية والاجتماعية قسم علوم الاعلام والاتصال، جامعة قاصدي مرباح – ورقلة، جزائر، ٢٠٢١، ص ٣٢.

(٥) د. مهند حميد عبيد، انعكاس التزييف العميق في الاعلام الرقمي على مصداقية مصادر الاخبار التلفزيونية، بحث منشور في مجلة دراسات والبحوث الإعلامية (M.S.A.R)، مجلد٣، عدد١٠، سنة ٢٠٢٣، ص٢٦٥.

(٦) د. محمود زكي زيدان، المواجهة الجنائية للاستخدام غير المشروع لتقنية التزييف العميق(دراسة مقارنة)، مرجع سابق، ص٢١.

ومن خلال ما تقدم من تعريفات حول جريمة التزييف العميق، يمكن ان نعرفها بدورنا بأنها(هي تقنية من تقنيات الذكاء الاصطناعي التي يستعملها الجاني من اجل العمل على خلق وانتاج محتوى مزيف للشخص المستهدف من خلال استخدام الحاسوب والاعتماد على تقنية التعلم الآلي والتعلم العميق من اجل انتاج مقاطع فيديو او صور او تسجيلات صوتية مزيفة للشخص الضحية وهو يقوم بأفعال أو حركات أو اصوات لم يقوم بها في الحقيقة واظهارها للجمهور من خلال نشرها بأي وسيلة من وسائل النشر، وتكون على مستوى عالي من الدقة والاحترافية، اذ يصبح من الصعب التمييز بين الحقيقة والمزيف، من اجل أهداف أو غايات محدده يسعى اليها الجاني من خلال المحتوى المزيف).

الفرع الثاني

خصائص جريمة التزييف العميق

تعد جريمة التزييف العميق من الجرائم المستحدثة التي تقع باستخدام تقنيات الذكاء الاصطناعي، ولها عدة خصائص ومن أهمها:

١- جريمة التزييف العميق من الجرائم المستحدثة: تعد جريمة التزييف العميق من الجرائم الحديثة التي ظهرت بتطور الوسائل الالكترونية والرقمية والتي تقوم على تزييف مقاطع الفيديو والصور للأشخاص ايان كانت طبيعته سواء كان المحتوى مرئي أو صوتي ويتم التلاعب بهذا المحتوى من خلال شبكات الخصومة التوليدية التنافسية من أجل انتاج المقاطع المزيفة(١).

٢- جريمة التزييف العميق سلوك متصل بالذكاء الاصطناعي: يعد الذكاء الاصطناعي بأنه جزء من علم الحاسوب ويكون الهدف منه هو جعل الكمبيوتر أو الالة التي تقوم بالبرمجة مثل الانسان، سواء في تفكيره أو تصرفاته أو حل لمشكلاته، وممارسته لكافة الحياة اليومية، وذلك من خلال دراسات تجري على الانسان وتستخلص منها نتائج تساعد في تفسير سلوك الانسان وبرمجة ذلك لتطبيقه الالة(٢).

٣- يتم اجراء معالجة كبيرة للمعلومات والبيانات: تتطلب جريمة التزييف العميق كميات ضخمة من البيانات والمعلومات حول الشخص الضحية او المستهدف من اجل تدريب النماذج العميقة من اتمام

(١) محمد ابراهيم العليلي، المواجهة الاجرائية للجرائم الالكترونية (دراسة مقارنة)، اطروحة دكتوراه، كلية القانون، جامعة الشارقة، الامارات العربية المتحدة، ٢٠٢٣، ص١٩.

(٢) محمد علي أبو علي، المسؤولية الجنائية عن أضرار الذكاء الاصطناعي، ط ١، دار النهضة العربية، مصر، ٢٠٢٤، ص ٢٢.

عملية التزييف العميق، ويتم الحصول على المعلومات والبيانات للأشخاص من صور ومقاطع فيديو او حتى تسجيلات صوتية من خلال عملية التبادل للرسائل التي تحصل بين الافراد وتحتوي على صور أو مقاطع فيديو أو تسجيلات صوتية، او انه يتم الحصول عليها من الصفحات الرسمية للأشخاص الذين يقومون بإتاحة بياناتهم ومعلوماتهم على صفحاتهم الرسمية، مما ارتكبت هذه الجريمة في اول ضهورها على المشاهير والفنانين والشخصيات العامة والمعروفة[١].

٤- الدقة الواقعية والعالية في التزييف العميق: تتجلى الدقة الواقعية والعالية في جريمة التزييف العميق من خلال البرامج والخوارزميات التي تستعمل في التزييف، ويتم ذلك من خلال المنافسة بين خوارزميتين، حيث تقوم الخوارزمية الاولى بنسخ مقطع فيديو متطابق عدة مرات من خلال استرداد وجه خارجي اليه، بينما تعمل الخوارزمية الثانية على كشف مدى جودة مقطع الفيديو او الصورة او التسجيل الصوتي الذي تم انشاؤها بواسطة الخوارزمية الاولى وهذا ما يطلق عليه (GAN)، اي شبكات الخصومة التوليدية التنافسية ومن خلال ذلك ان هدف تقنية التزييف العميق هو انشاء مقاطع فيديو او صور او انتاج تسجيلات صوتية مزيفة لغاية وهدف يسعى اليه الجاني من اجل تحقيقه[٢].

المطلب الثاني

انواع التزييف العميق واثارة

ان جريمة التزييف العميق من الجرائم التي تقع على المحتوى المرئي والصوتي، كما ان لهذه التقنية العديد من المخاطر والاثار على الافراد والمجتمعات والدول[٣]، وعلية سوف نبين انواع المحتوى المزيف تزيفاً عميقاً، والاثار التي تترتب على جريمة التزييف العميق.

(١) د. أشرف سيد أبو العلا، المواجهة الجنائية لمخاطر تقنية الديب فيك (Deep fake) واثرها على حجية الادلة الرقمية في الاثبات الجنائي (دراسة تحليلية مقارنة)، ط ١، دار النهضة العربية، مصر، ٢٠٢٤، ص٢٠-٢١.

(٢) د. باسم محمد فاضل، التحديات القانونية لتقنية التزييف العميق (DEEP FAKE)، دراسة تحليلية مقارنة، ط١، دار الفكر الجامعي، مصر، ٢٠٢٥، ص ٤٥.

(٣) غدير مجادب الرويلي، المسؤولية الجنائية عن إساءة استخدام تقنية التزييف العميق (دراسة مقارنة)، رسالة ماجستير، كلية العدالة الجنائية، جامعة نايف العربية للعلوم الامنية، السعودية،٢٠٢٣، ص١٦.

الفرع الاول

انواع المحتوى المزيف تزيفاً عميقاً

ان جريمة التزييف العميق من الجرائم المستحدثة التي تقع على المحتوى المرئي والمحتوى الصوتي من خلال انتاج أو اصطناع صور أو تسجيلات صوتية أو مقاطع فيديو مزيفة تبدو وكأنها حقيقية، وعلية ينقسم المحتوى الى:

اولاً: المحتوى المرئي: يقصد بالمحتوى المرئي "هو استخدام تقنية التزييف العميق في إنشاء الصور ومقاطع الفيديو"، وذلك من خلال عملية تغيير الوجه ويتم تغيير الوجه من خلال استخدام خوارزميات التشفير وفك التشفير من اجل تركيب الخريطة الرقمية لوجه فرد ما على وجه فرد اخر(١)، من خلال طريقتين وهما:

١- تزييف الوجوه: يتم تبديل عملية تزييف الوجوه من خلال استبدال وجه شخص بوجه شخص اخر في فيديو أو صورة من خلال استخدام خوارزميات التشفير وفك التشفير، مما تعمل هذه الخوارزميات على وضع خريطة رقمية لوجه شخص معين على وجه شخص اخر، من خلال دراسة تعابير الوجه لدى الفردين المختلفين ومن ثم تقوم باكتشاف التشابه بينهما واختصار الصفات المشتركة ومن بعدها ضغط الصور، على ان يتم تدريب خوارزمية فك التشفير من خلال استعادة الوجوه من الصور المضغوطة، وانه لطالما الوجهين مختلفين فيتم برمجة الخوارزمية الاولى لاستعادة وجه الفرد الثاني، ولكي يتم تزييف الوجهين يجب تزويد خوارزمية فك التشفير ببيانات الصورة المشفرة المختصة بالوجه الاخر(٢).

٢- التلاعب بالوجه: تتم عملية التلاعب بالوجه من خلال استخدام الشبكات التوليدية التنافسية، من خلال العمل على استبدال وتغيير تعابير الوجه ومطابقة الشفاه، من خلال استخدام خوارزمية الاولى والتي تسمى التوليد التي يتم تزويدها بمجموعة من البيانات العشوائية من اجل تحويل هذه البيانات الى صورة، ومن ثم تضاف هذه الصورة المصطنعة من ضمن سلسلة الصور الحقيقية، وبعدها يتم ادخالها

(١) د. الاسد صالح الاسد، المخاوف الاخلاقية من الاستخدامات السلبية لتقنيات الذكاء الاصطناعي- تقنية التزييف العميق نموذجا، بحث منشور في مجلة الدراسات الاعلامية، مجلد ٦، عدد ٢، سنة ٢٠٢٢، ص٣٧٦.

(٢) د. باسم محمد فاضل، التحديات القانونية لتقنية التزييف العميق، مرجع سابق، ص ٥٤.

الى الخوارزمية الثانية المعروفة باسم خوارزمية التمييز، من اجل انتاج صور تنتج جديدة بعد تنفيذ عدد من الملاحظات والدورات، تبدأ الخوارزمية بتصنيع وجوه حقيقية تماماً لأشخاص مزيفين[١].

ثانياً: المحتوى الصوتي: يقع التزييف العميق على المحتوى الصوتي من خلال(تزييف الصوت)، من خلال استخدام خوارزميات الذكاء الاصطناعي من اجل تركيب صوت او تعديله من خلال إنشاء ملف صوتي يتضمن حديثاً مزيفاً بنفس صوت الشخص لكنه لم يقله في الحقيقة، او من خلال التحكم بنبرة صوت الشخص ونغمته لإظهار شعور او سلوك غير حقيقي [٢].

اذ تقع جريمة التزييف العميق من خلال عملية جمع الفيديوهات والملفات الصوتية والصور ومن ثم العمل على تزيفها بدقة بواسطة التعلم الألي، كما تكون كافة اقسام التزييف العميق ممكنة من تغيير الوجوه أو تبديلها بوجه فرد اخر أو من خلال ضبط فم المتحدث في ملف صوتي مختلف عن الصوت الاصلي الحقيقي أو من اجل استنساخ الاصوات من خلال اخذ نسخة من الصوت الاصلي من اجل العمل على تزييفه من اجل اساءه استخدامه او ليقول اشياء لم يقلها الفرد في الواقع، لذلك تعد جريمة التزييف العميق من الجرائم التي تكون لها مخاطر واثار كبيرة، لأنها تشوه سمعة وتلعب بالحقائق التي تظهر للعلن[٣].

ومن الامثلة على جرائم التزييف الصوتي، اذ نشرت مجلة " فوربس (Forbes)"[٤]، في وثيقة محكم انه تمت عملية سرقة بنك دبي الاسلامي في الامارات بداية سنة ٢٠٢٠، من خلال عملية معقدة، حيث تلقى مدير البنك مكالمة هاتفية من مدير اخر معروف لدية، وزعم المدير الاخر ان الشركة كانت على وشك إجراء عملية استحواذ وتحتاج من البنك السماح لها بالقيام ببعض التحويلات المالية التي تبلغ قيمتها (٣٥) مليون دولار، من خلال إظهاره لمدير البنك رسائل بريد الكتروني من المحامي والمسؤول عن الصفقة، وكل شيء كان امراً طبيعياً ولا يوجد ما يدعو للشك، لذا اكمل مدير البنك جميع التحويلات

(١) غدير مجادب الرويلي، المسؤولية الجنائية عن إساءة استخدام تقنية التزييف العميق، مرجع سابق،ص١٨.

(٢) البرنامج الوطني للذكاء الاصطناعي(دليل التزييف العميق) لسنة ٢٠٢١، ص١٠.

(٣) د. باسم محمد فاضل، التحديات القانونية لتقنية التزييف العميق، مرجع سابق، ص٥٥.

(٤) فوربس(Forbes) هي شركة من شركات النشر والاعلام في الولايات المتحدة الامريكية.

المالية ولم يكون لدية اي علم بأنه كان جزءاً من عملية احتيال عملاقة، اذ استخدم المحتالون تقنية التزييف العميق من اجل تزييف صوت المدير من خلال استنساخ خطاب المدير[١].

الفرع الثاني

اثار جريمة التزييف العميق

ان قدرة تقنية التزييف العميق على صنع فيديوهات وصور وتسجيلات صوتية متقنة بشكل مقنع للجميع، مما جعل هذا الامر ان تقنية التزييف العميق سلاحا فعالا عندما يساء استخدامه من قبل المجرمين المعلوماتيين، من خلال استخدامه من اجل الاساءة الى سمعة الاشخاص وبث الشائعات والافكار المتطرفة والترويج لها سواء كانت اجتماعية أو سياسية أو دينية، وهذا الامر يثير الجدل واللغط مما يؤدي الى حدوث اضطرابات أمنية وسياسية واقتصادية واجتماعية وثقافية، وجميع هذه الاضطرابات تؤدي الى تهديد أمن المجتمع والسلام العالمي[٢]، مما يكون لهذه التقنية عدة أثار خطرة ومضرة ومنها:

١- **التشكيك في المصداقية:** تعد المصداقية شيء اساسي في التعامل مع كل شيء الا انه مع تطور العالم الرقمي والتكنولوجي وازدياد استعمال الانترنت ادى ذلك الى التقليل من المصداقية بين المجتمعات، لان اصبح التمييز بين الفيديو الحقيقي والفيديو المزيف في غاية الصعوبة، اذ ان تقنية التزييف العميق تعمل على تعديل وتحرير وخلق مقاطع مرئية أو صوتية تبدو وكأنها حقيقية، مما ينعكس اثر ذلك على جميع الفيديوهات والصور المنشورة على مواقع التواصل الاجتماعي، لان ذلك سوف يخلق الكثير من الجدل عند انتشار اي فيديو حتى لو كان صحيحاً، وهذا ما يخلق مشكلة كبيرة في ثقة المعلومات التي تنشر على وسائل الاعلام والصحافة ومواقع التواصل الاجتماعي[٣]، ومن الامثلة على ذلك، عندما قام حزب في أمريكا على خلق ازمة سياسية من خلال نشر مقطع فيديو لدونالد ترامب، وهو يسخر من قرارات بلجيكا السياسية، وعلى الرغم من ان هذا المقطع لم يكن على درجة عالية من التزييف العميق، كما انه ذكر في نهاية المقطع على لسان ترامب، بالإضافة ان الجو المناخي الموجود في المقطع كان

(١) انظر موقع جزيرة نت، موقع ويب اخباري تابع لقناة الجزيرة على الرابط ، https://www.aljazeera.net ، تاريخ ووقت الزيارة٢٣/١٠/٢٠٢٤، ١٠:٠٠م.

(٢) د. علي مولود فاضل، سيف عدنان عباس، التزييف العميق لغة الذكاء الاصطناعي في حروب السيبران الإعلامية، ط١، دار امجد للنشر والتوزيع، الاردن، ٢٠٢٢، ص٣٤.

(٣) د. عبد الناصر ونوس، لجين خضور، بعض تطبيقات تقنية التزييف العميق(الديب فيك) وتوظيفها في التسويق والترويج المعاصر، بحث منشور في مجلة جامعة دمشق للعلوم الهندسية، مجلد ٣٩، عدد٢، ٢٠٢٣، ص١٠.

واضح انه مزيف تماما، الا انه اخذ صدى واسع عند انتشاره على مواقع التواصل الاجتماعي فيسبوك وتويتر، مما اثار الجدل بسبب انتشاره كما ان مواقع التواصل الاجتماعي اصبحت بيئة خصبة لانتشار الشائعات والاخبار سواء كانت صحيحة أو غير صحيحة، فكل هذا يهدد النسيج الاجتماعي والثقافي والفكري[١].

٢- **التسبب بأزمات سياسية وامنية:** ان استخدام تقنية التزييف العميق لتهديد الوضع السياسي والدولي من خلال التضليل السياسي وخداع الجمهور بخلق اكاذيب وشع الفتن واثارة التوترات والسياسية والامنية، مثل القيام بعمل فيديو مزيف يظهر فيه رئيس دولة ما يدعو الى اعلان الحرب على دولة أخرى أو عمل فيديو مزيف لشخصية دينية ينكل او يقلل من قيمة الطائفة او الديانة الاخرى[٢]، مما يتسبب هذا التزييف العميق بالتحريض على العنف من خلال اثاره النعرات الطائفية او ان الهدف منه التأثير على الامن الوطني والقومي كالتأثير على الحملات الانتخابية او القيام بالتصفية السياسية لبعض الخصوم او في حال تم استخدام التزييف العميق من قبل العصابات الاجرامية والغرض منه الابتزاز والتشهير والحاق الضرر بالأخرين، وهذا الامر يؤدي اثاره القلق السياسي داخل المجتمع ويثير العديد من المخاوف في المستقبل[٣].

٣- **خطر التزييف العميق على الادلة الرقمية:** يعد الدليل الرقمي من ابرز الادلة الذي ظهر مع ظهور فكرة الجرائم المعلوماتية، اذ ان هذه الجرائم يتعذر اثباتها في اغلب الحالات الا في حالة وجود دليل رقمي، الذي يعد من ضمن الادلة التي تكون ذات طبيعة معقدة وصعبة[٤]، لكن من ظهور التزييف العميق الذي طالت اثارة ومخاطرة جميع مجالات الحياة ومنها الادلة الرقمية، لأنه بعد ظهور تقنية التزييف العميق وتطورها اصبح في الوقت الحاضر الاخذ بجميع الادلة الرقمية او الاستناد عليها في الدعوى بصورة عامة، لأنه اصبح من الصعب التمييز بين الادلة الحقيقية والمزيفة، اذ انه من الممكن

(١) د. رضا ابراهيم عبد الله البيومي، الحماية القانونية من مخاطر تطبيقات التزييف العميق في الفقه الاسلامي والقانون الوضعي (دراسة تحليلية مقارنة)، عدد خاص المؤتمر العلمي الدولي الثامن – التكنولوجيا والقانون، منشور في مجلة روح القوانين، مجلد٣٥، عدد١٠٢، ٢٠٢٣، ص٨٤٣-٨٤٤.

(٢) محمد ستار جبار، التزام الإدارة بمنع الاشاعة الماسة بسير المرافق العامة، بحث منشور في مجلو ميسان للدراسات القانونية المقارنة، كلية القانون، جامعة ميسان، العدد ٩، المجلد ١، ٢٠٢٤، ص ٤٢٧-٤٢٨

(٣) د. علي مولود فاضل، سيف عدنان عباس، التزييف العميق، مرجع سابق، ص٣٤- ٣٥.

(٤) غدير مجادب الرويلي، المسؤولية الجنائية عن إساءة استخدام تقنية التزييف العميق، مرجع سابق،ص٥٦.

تزييف البصمات الصوتية أو الصور أو الفيديوهات من خلال التلاعب بها من اجل تبرءه شخص او ادانته[١].

٤- انتهاك حقوق الملكية الفكرية والحقوق المجاورة: ان جريمة التزييف العميق تعمل على انتهاك حقوق الملكية من خلال انتاج محتوى مرئي مزيف مثل الصور والفيديوهات للمشاهير والفنانين ومنتجي الافلام من دون موافقتهم، مما يتسبب بمشاكل لهم سواء، من خلال انتهاك حقوق النشر والطبع[٢].

٥- تدمير الحياة الخاصة للأفراد من خلال عملية الانتقام الاباحي والابتزاز الالكتروني: يعد الحق بالخصوصية من الاشياء اللصيقة بالإنسان وهذا الحق عام ومطلق لكل انسان ويجب على الجميع احترام هذا الحق ويصنف من ضمن الحقوق الغير مالية لان هذا الحق ليس له قيمة مادية، وان الغرض الاساسي هو ضمان حماية المصالح المعنوية وجوهر هذا الحق يدور حول الخصوصية، وان حق الفرد في حفظ خصوصيته يعد من ضمن الحقوق الاساسية التي كفلتها دساتير دول العالم، اذ يعد انه شرط ضروري لحماية حقوق اخرى مثل الحق في الشرف والسمعة والكرامة والحرية الشخصية والدين والرأي ومعلومات وبيانات الشخص الخاصة به كل هذه تعتبر من الحقوق التي تدخل في خصوصية الانسان ولا يجوز مساسها أو التجاوز والاعتداء عليها[٣].

المبحث الثاني

التكييف القانوني لجريمة التزييف العميق ودوافع ارتكابه

ان المقصود بالتكييف القانوني هو نشاط قضائي منطقي يستند على اسس ثابتة ويستعين بوسائل شتى، جوهرة مطابقة الواقعة بالنص القانوني الذي يحكمها ومحصلته تحديد الوصف القانوني السليم للواقعة، وغايته الفصل في موضوع الدعوى[٤].

(١) محمد مصطفى صلاح عبد الحميد، التزييف الرقمي وأثره على حجية الأدلة الرقمية في الدعاوى الجنائية (دراسة فقهية مقارنة)، بحث منشور مجلة الشريعة والقانون، كلية الشريعة والقانون، جامعة الازهر، القاهرة، عدد٤٠، ٢٠٢٢، ص٨٥٦- ٨٥٧.

(٢) د. براء منذر كمال، د. مريفان مصطفى رشيد، دور القانون في حماية حقوق الإنسان من التزوير العميق، مرجع سابق، ص١٧.

(٣) د. أشرف سيد أبو العلا، المواجهة الجنائية لمخاطر تقنية الديب فيك، مرجع سابق، ص٣٨.

(٤) ميادة محمد أحمد، التكييف القانوني للوقائع في الدعوى الجزائية (دراسة مقارنة)، اطروحة دكتوراه، كلية الحقوق، جامعة الموصل، العراق، ٢٠٢٠، ص ١٢.

ان التشريعات الجنائية العامة والخاصة في التشريعات محل المقارنة وفي قانون العقوبات العراقي جاءت خالية من أي معالجة قانونية لجريمة التزييف العميق، نظرا لكونها من الجرائم المستحدثة التي ظهرت الى العالم المادي بعد صدور القانون، الا ان هذا لا يعني أن يكون التزييف العميق سلوكا مباحاً، لذا يجب البحث في النصوص القانونية التقليدية التي يمكن تطبيقها على جريمة التزييف العميق في حالة توفر الشروط القانونية التي تسمح بالتطبيق، وان الغرض من البحث عن التكييف القانوني لجريمة التزييف العميق وفقاً للنصوص العقابية التقليدية هو من اجل التصدي لمشكلة التزييف العميق والحد من اثارة السلبية على جميع مجالات الحياة المختلفة، لذا تحمل جريمة التزييف العميق الكثير من الاوصاف الجرمية[١].وعليه سوف نبين في هذا المبحث التكييف القانوني لجريمة التزييف العميق في المطلب الاول، الاول، وفي المطلب الثاني سوف نبين دوافع ارتكاب جريمة التزييف العميق.

المطلب الاول

التكييف القانوني لجريمة التزييف العميق

تعد جريمة التزييف العميق من الجرائم المستحدثة التي ظهرت الى العالم المادي اليوم، اذ نجد خلو القانون الخاص بمكافحة الجرائم المعلوماتية ، وكذلك قانون العقوبات في مصر والامارات من اي معالجة قانونية واضحة وصريحة، لكونها ظهرت بعد صدور القوانين الخاصة، كما ان العراق يعد من الدول التي لم يوجد لديها تشريع خاص ينظم ويجرم الجرائم المعلوماتية وجرائم الذكاء الاصطناعي، وهذا ما يقتضي الضرورة بالإسراع بإقرار قانون خاص بمكافحة الجرائم المعلوماتية وان يكون هناك تجريم واضح لجريمة التزييف العميق، الا ان الجهات القضائية في العراق والدول محل المقارنة عملت على تكييف جريمة التزييف العميق وفقاً لنشاط الجرمي للجاني[٢]، لان الغرض من تكييف جريمة التزييف العميق وفقاً للنصوص التقليدية يمكن من التصدي لمواجهة جريمة التزييف العميق والحد من ارتكابها واثارها السلبية على المجتمع والافراد.

(١) د. براء منذر كمال، د. نورس رشيد طه، التصدي الجنائي للابتزاز الإلكتروني، ط١، دار المسلة، بغداد، العراق، ٢٠٢٤، ص ٤٩.

(٢) محمد علي سالم، حسون عبيد هجيج، الجريمة المعلوماتية، بحث منشور في مجلة جامعة بابل للعلوم الانسانية، مجلد١٤، عدد٢، ٢٠٠٧، ص٩٠.

الفرع الاول

تكييف التزييف العميق وفق جريمة الابتزاز الالكتروني

يمكن تكييف فعل التزييف العميق بأنه جريمة ابتزاز الكتروني اذ يعرف الابتزاز الالكتروني بأنها "عملية تهديد أو تخويف يقوم بها الجاني من اجل التأثير أو تهديد الضحية من خلال نشر مقاطع فيديو أو صور أو معلومات سرية تخص المجني عليه أو عائلته، من خلال مواقع التواصل الاجتماعي مقابل دفع مبالغ مالية أو اجبار الشخص الضحية على القيام بأفعال غير مشروعة أو مشروعة"[١]، اي انه في حال انطباق شروط تطبيق نص جريمة الابتزاز الالكتروني على فعل التزييف العميق يمكن تكييفه بأنه ابتزاز الكتروني، فيجتمع فعل التزييف العميق مع جريمة الابتزاز الالكتروني من خلال قيام الجاني بتزييف الصور أو التسجيلات الصوتية ومقاطع الفيديو للشخص الضحية بشكل مخل بالحياء او كان المحتوى المزيف اباحي او جنسي، ويعمل الجاني على ابتزاز المجني عليه من خلال تهديده بعرض او نشر المحتوى المزيف تزيفاً عميقاً على مواقع التواصل الاجتماعي مقابل الحصول على مال او ان يطلب من المجني عليه القيام بعمل او الامتناع عن عمل[٢].

ومن اجل تكييف فعل التزييف العميق وفق جريمة الابتزاز الالكتروني، فأن ذلك يتطلب مرتكزات مادية، والتي تتمثل في (فعل الاعتداء او نشاط الجاني)[٣]، ويتمثل نشاط الجاني من خلال قيامة بجمع الصور والفيديوهات للشخص الضحية، ومن ثم العمل على تزيفها من خلال استخدام الحاسوب الالي وتقنيات الذكاء الاصطناعي من اجل انتاج محتوى مزيف للشخص المبتز، و (النتيجة الجرمية)، والتي تتمثل في الاثر القانوني الذي يترتب نتيجة فعل الجاني وهو ابتزاز المجني عليه بنشر الصور او الفيديو المزيف عبر شبكة الانترنت، مما تترك هذه النتيجة في نفس الضحية الخوف والرعب مما يضطر الى القيام بتنفيذ ما يطلبه الجاني سواء مبالغ مالية او اقامة علاقات غير مشروعة، و (العلاقة السببية)، التي تتمثل في الرابطة التي تربط بين سلوك الجاني المتمثل في الحصول على الصور والفيديوهات الخصة

(١) رنا حكمت عباس، الابتزاز الالكتروني، بحث منشور في مجلة لارك للفلسفة واللسانيات والعلوم الاجتماعية، مجلد١، عدد٤٤، كلية الآداب، قسم علم الاجتماع، جامعة واسط، العراق، ٢٠٢٢، ص٤٧٢.

(٢) روان يعقوب سعيد الزيان، الابتزاز الالكتروني في التشريع الفلسطيني (دراسة مقارنة بأحكام الفقه الإسلامي)، رسالة ماجستير، كلية الشريعة والقانون، الجامعة الاسلامية بغزة، فلسطين، ٢٠٢٣، ص ١٩-٢٠.

(٣) د. مؤيد جبار محمد، التطويع القضائي للقواعد الجزائية الماد تطبيقها عند غياب التشريع الجنائي الخاص بالجرائم المستحدثة في العراق أنموذجا، بحث منشور في مجلو ميسان للدراسات القانونية المقارنة، كلية القانون، جامعة ميسان، العدد ١٠، المجلد ١، ٢٠٢٤، ص ٦٠٩

بالضحية والعمل على تزييفها من اجل استغلال المجني عليه من ابتزازه من خلال تحقيق اهداف معينة يسعى اليها الجاني من خلال هذا السلوك الجرمي[١]، اما المرتكزات المعنوية، فأنها تتمثل في العلم والارادة، من حيث علم الجاني يجب ان يعلم الجاني بكل العناصر التي تساهم في ارتكاب جريمة التزييف العميق، اي انه يجب ان يكون على علم بأنه يجمع معلومات وبيانات خاصة بشخص ما من دون علمه من اجل العمل على تزييفها من خلال استخدام الاجهزة والتقنيات الذكية من اجل ابتزاز الشخص بهذا المحتوى المزيف من اجل الحصول على غاية ما، اي ان يكون لدية علم بكل عناصر الجريمة ورحب بالنتيجة الجرمية كأثر لفعلة الجرمي، اما الارادة فأنها تتمثل في ارادة الجاني بأراده السلوك الجرمي واراده النتيجة الجرمية، اي ان اراده الجاني اتجهت الى ابتزاز المجني عليه من خلال تهديده بنشر المحتوى المرئي او الصوتي المزيف من اجل ارغام الضحية على تنفيذ طلبات الجاني[٢].

ان المشرع المصري قد عاقب على جريمة الابتزاز الالكتروني بموجب مواد محددة ومنها (٣٠٨، ٣٢٧)[٣]، في قانون العقوبات المصري رقم (٥٨) لسنة ١٩٣٧ المعدل، كما انه في قانون مكافحة جرائم تقنية المعلومات رقم (١٧٥) لسنة٢٠١٨ في المواد (٢٥، ٢٦)[٤]، اذ نجد ان المشرع المصري بموجب هذه المواد قد عاقب على فعل الابتزاز الالكتروني بعقوبات صارمة تصل الى السجن المؤبد او الحبس في حال تهديد الاشخاص بإفشاء امور تخدش الشرف والسمعة، اي انه في حال تكييف فعل التزييف العميق فأنه يكيف وفق هذه المواد من قانون مكافحة جرائم تقنية المعلومات، لان هذه جرائم تتعلق بالاعتداء على حرمة الحياة الخاصة للأفراد في ظل بيئة معلوماتية ومن دون وجه حق مشروع.

اما المشرع الاماراتي فأنه قد عاقب على الابتزاز الالكتروني في ضوء قانون مكافحة الشائعات والجرائم الالكترونية رقم (٣٤) لسنة٢٠٢١ المعدل في المادة (٤٢/فقرة١)[٥]. اما المشرع العراقي قد كييف فعل الابتزاز الالكتروني وفق المواد (٤٣٠- ٤٣٢) من قانون العقوبات العراقي، وان هذه المواد الموجودة في النصوص العقابية جاءت بخصوص الجرائم التقليدية وفي حال ارتكاب جريمة التزييف العميق سوف

(١) دعاء سليمان عبد القادر التميمي، جريمة الابتزاز الالكتروني (دراسة مقارنة)، رسالة ماجستير، كلية الحقوق، جامعة القدس أبوديس، القدس، فلسطين،٢٠١٩، ص١٣- ١٨.

(٢) باقر غازي حنون الدراجي، المسؤولية الجنائية الناشئة عن الابتزاز الإلكتروني (دراسة مقارنة)، رسالة ماجستير، كلية القانون، جامعة البصرة، العراق،٢٠٢٠، ص ٦٩-٧٣.

(٣) المواد (٣٠٨، ٣٢٧) من قانون العقوبات المصري رقم (٥٨) لسنة١٩٧٣ المعدل.

(٤) المواد(٢٥، ٢٦) من قانون مكافحة جرائم تقنية المصري رقم(١٧٥) لسنة ٢٠١٨.

(٥) المادة (٤٢/ فقرة١) من قانون مكافحة الشائعات والجرائم الالكترونية الاماراتي رقم (٣٤) لسنة ٢٠٢١ المعدل.

تكييف وفقا لجريمة التهديد، وهذا يعتبر قصور تشريعي يجب تلافيه من خلال تشريع خاص بالجرائم المعلوماتية كما هو الحال في الدول الاخرى التي شرعت قوانين خاصة لهذه الجرائم من اجل مواجهتها ومكافحتها .

ومن تطبيقات ذلك حكم محكمة جنح الحلة قرارها المرقم (١٢١٣/ج/٢٠٢٣) والمتضمن الحكم على المدان بالحبس البسيط لمدة ستة اشهر استناداً لأحكام المادة (١/٤٣٣) من قانون العقوبات العراقي، الا أن وكيل المميز لم يقتنع بالقرار المذكور، مما بادر الى الطعن به امام محكمة استئناف بابل بصفتها التمييزية بتاريخ ٢٠٢٣/٥/١٤ بالدعوى المرقمة بالعدد (٩٢٦/ت/ج/٢٠٢٣) "ولدى التدقيق والمداولة فقد وجدت المحكمة ان الحكم غير صحيح ومخالف لأحكام القانون، كون محكمة الموضوع قد اخطأت في الوصف القانوني للحادث وجعلة وفقاً للمادة(١/٤٣٣) من قانون عقوبات عراقي، لأنه تبين من خلال وقائع الدعوى وادلتها واقوال المشتكية واقوال شهود الاثبات بشهادتهم العيانية بالحادث واستجواب المتهم الذي نتج عنه اعترافاً بالحادث ومحاضر ضبط الرسائل والمقطع الصوتية على مواقع التواصل الاجتماعي التي تبين انها تعود للمتهم والمشتكية، بالإضافة الى تقرير الخبرة الوارد من مديرية تحقيق الادلة الجنائية شعبة الجرائم الالكترونية المتضمن وجود مقاطع صوتية وصور شخصية تعود للمشتكية، اذ قام المتهم بابتزازها من خلال طلب مبالغ مالية وجهاز هاتف نقال والا سوف ينشر صورها على مواقع التواصل الاجتماعي، اذ تبين لدى المحكمة بعد التدقيق والمداولة ان هذه الجريمة المرتكبة من قبل المتهم بانها جريمة ابتزاز الالكتروني، من خلال توفر اركان جريمة الابتزاز الالكتروني من خلال الواقعة المعروضة من خلال توفر الركن المادي بعناصر السلوك الاجرامي والنتيجة الجرمية والعلاقة السببية، اضافة للركن المعنوي المتمثل بالقصد الجنائي بعنصري العلم والارادة، من اجل استمرار العلاقة له مع المشتكية وطلب مبالغ مالية وهاتف نقال لاحقا، ولثبوت جميع هذه الافعال بالأدلة والشهود، ولعدم صدور قانون مكافحة الجرائم المعلوماتية في العراق، ولان قواعد قانون العقوبات هي المطبقة حالياً، لذا ان التكييف القانوني السليم لفعل المتهم ينطبق وفق احكام المادة(٤٣٠) من قانون العقوبات العراقي، والداخلة من ضمن اختصاص محكمة جنايات بابل حسب الاختصاص الوظيفي، واشعار محكمة جنح الحلة بذلك"[١].

(١) قرار محكمة استئناف بابل بصفتها التمييزية، بالعدد (٩٢٦/ت/ج/٢٠٢٣)، بتاريخ ٢٠٢٣/٥/١٤ (منشور).

الفرع الثاني

تكييف التزييف العميق وفق جريمة التهديد

يمكن تكييف فعل التزييف العميق بأنه جريمة تهديد، في حال انطباق شروط تطبيق نص جريمة التهديد عليه، فيجتمع فعل التزييف العميق مع التهديد في حال قيام الجاني بتهديد المجني عليه وترويعه من خلال نشر الصور أو الفيديوهات المزيفة تزييفاً عميقاً والتي قد يكون الجاني حصل عليها من خلال تهكير موقع المجني عليه وحصل على المعلومات الخاصة بالضحية أو انها حصل عليها من خلال الثقة الموجودة بين الجاني والمجني عليه، وان الغرض من تزييف الصور او الفيديوهات للشخص الضحية هو من اجل بالقيام بفعل أو الامتناع عن فعل مقصودا به ذلك، ومن اجل تكييف فعل التزييف العميق وفق جريمة التهديد، فان ذلك يتطلب مرتكزات مادية، والتي تتمثل في (فعل الاعتداء او السلوك)، اي قيام الجاني بأي سلوك مخالف للقانون سواء كان إيجابيا أو سلبيا[١]، و (النتيجة الجرمية) والتي تتمثل في الاثر القانوني الذي يترتب نتيجة سلوك الجاني سواء كانت النتيجة مباشرة او محتملة له والتي تتمثل في جريمة التزييف العميق هو القاء الفزع والخوف والرعب في نفس المجني عليه من خلال تهديده بنشر المحتوى المرئي او الصوتي المزيف تزيفا عميقا، و (العلاقة السببية) اي ان يكون هناك ارتباط وثيق بين سلوك الجاني والنتيجة الجرمية، اما المرتكزات المعنوية، فأنها تتمثل في (العلم والارادة)، من ناحية علم الجاني يجب ان يكون لدية علم بماديات جريمة التزييف العميق، بأنه يقوم بسلوك مخالف للقانون وعلمة بالنتيجة الجرمية التي سوف تترتب على فعلة وانه ارادها ورحب بها كأثر لفعلة الجرمي، اما الارادة اي انه الجاني قد توجه بإرادته الى تحقيق النتيجة الجرمية الناجمة عن فعلة الجرمي، لذا تعد جريمة التزييف العميق من الجرائم العمدية[٢].

ان المشرع المصري في قانون مكافحة جرائم تقنية المعلومات رقم (١٧٥) لسنة ٢٠١٨، لم ينص على جريمة التزييف العميق صراحة، كما انه لم ينص على جريمة التهديد الالكتروني، لكن في حال ارتكاب جريمة التزييف العميق، فأن القضاء المصري كيفها وفق جريمة التهديد المنصوص عليها في المادة (٣٢٧) من قانون العقوبات المصري رقم (٥٨) لسنة ١٩٣٧ المعدل[٣].

(١) نصت المادة (١٩/ فقرة٤) من قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل.

(٢) د. براء منذر كمال، د. نورس رشيد طه، التصدي الجنائي للابتزاز الإلكتروني، مرجع سابق، ص٥٠- ٥٢.

(٣) نص المادة (٣٢٧) من قانون العقوبات المصري رقم (٥٨) لسنة ١٩٣٧ المعدل.

كما أن المشرع الاماراتي لم ينص على تجريم التزييف العميق لكنه يمكن تكييف فعل التزييف العميق وفقاً لجريمة التهديد الالكتروني التي عاقب عليها المشرع في قانون العقوبات الاماراتي رقم (٣) لسنة ١٩٨٧ المعدل في المادة (٣٥١)، وفي قانون مكافحة الشائعات والجرائم الالكترونية رقم (٣٤) لسنة٢٠٢١ المعدل على تجريم التهديد الالكتروني في المادة (٤٢/فقرة٢)[١]. اما المشرع العراقي فأنه في حال ارتكاب فعل التزييف العميق يمكن تكييف هذا الفعل وفقا لجريمة التهديد في قانون العقوبات العراقي من المادة (٤٣٠)[٢]، كما انه جرم التهديد في مشروع قانون مكافحة الجرائم الالكترونية لسنة ٢٠١٩، في المادة (٦) التي نصت على انه "كل من استخدم شبكة المعلومات او احد أجهزة الحاسوب بقصد تهديد شخص اخر من اجل حملة على القيام بفعل او الامتناع عنه ولو كان هذا الفعل مشروعا"[٣].

ومن تطبيقات ذلك صدقت محكمة التميز الاتحادية العراقية في أحد قراراتها "حكم محكمة جنايات المثنى المرقم بالعدد ٥١٤/ج/٢٠١٨، والصادر بتاريخ ٢٠١٨/١٢/٢، الذي يقضي بسجن المتهم مدة خمس سنوات وشهر نتيجة لاختراقه الصفحة الشخصية والعائلية للمجني عليه وتهديدها بنشر الصور الشخصية والإساءة لها ومساومتها لها بإعطائه أرصدة بطاقات تعبئة ومبالغ مالية مقابل الامتناع عن نشر تلك الصور المستولى عليها"[٤].

الفرع الثاني

دوافع ارتكاب جريمة التزييف العميق

ان مجرمي جريمة التزييف العميق يختلفون عن مجرمي مرتكبي الجرائم التقليدية من حيث الاسباب والعوامل التي تدفع بهم الى ارتكاب هذه الجريمة، لان كل جريمة توجد خلفها دوافع واسباب تدفع بالشخص الجاني الى ارتكابها، اذ يعد الدافع أو الغاية أو الباعث كل هذه التعبيرات تكون لها دلاله اصطلاحية في القانون الجنائي، كلها تتصل بما يعرف بالقصد الجنائي في الجريمة، وهذه المسألة تثير جدلا فكرياً وقضائياً واسعاً، كما ان القاعدة القضائية تقرر أن الباعث ليس من عناصر القصد الجنائي،

(١) نص المادة (٤٢/فقرة٢) من قانون مكافحة الشائعات والجرائم الالكترونية رقم(٣٤) لسنة٢٠٢١ المعدل.

(٢) المواد (٤٣٠- ٤٣٢) من قانون العقوبات العراقي رقم (١١١) لسنة ١٩٦٩ المعدل.

(٣) المادة (٦) من مشروع قانون مكافحة الجرائم الالكترونية العراقي لسنة ٢٠١٩.

(٤) القرار ذو العدد (٣٧٥٨/ الهيئة الجزائية/٢٠١٩)، بتاريخ٢٠١٩/٣/١٧(غير منشور)، نقلا عن المرجع، د. براء منذر كمال، د. نورس رشيد طه، التصدي الجنائي، مرجع سابق، ص٥٥.

لان الباعث يعد هو "العامل الاساسي المحرك للإرادة الذي يوجه السلوك الإجرامي كالمحبة والشفقة والبغضاء والانتقام"[١]، لذا فان الدافع الذي يؤدي بالشخص الى ارتكاب جريمة التزييف العميق من خلال الحاسب الالي سواء كان بالإضافة أو الحذف أو التعديل، قد يكون خلفة مجموعة من الدوافع والاسباب التي تؤدي الى ارتكاب هذه الجريمة[٢]، وهذا ما سنبينه من خلال هذا الفرع، كالاتي:

١- **الدافع الجنسي أو العاطفي:** تعد الدوافع الجنسية من بين اخطر الدوافع التي تؤدي الى ارتكاب جريمة التزييف العميق وهو من اكثر الدوافع وقوعاً، من خلال قيام الجاني بدافع جنسي بالعمل على تزييف صورة او مقطع فيديو لفتاة من أجل القيام بعلاقة غير مشروعة معها او طلب مال وفي حال رفضت طلباته سوف يعمل على ابتزازها او تهديدها بنشر هذا المقطع المزيف مما تضطر الضحية الى الانتحار او الهروب من اهلها خوفاً من القتل وغسل العار، ويقع هذا الفعل خصوصاً الدولة العربية والاسلامية التي تكون قائمة على الدين الاسلامي وعلى النظام العام والآداب العامة بالإضافة الى العادات والتقاليد، كما ان أغلب ضحايا هذه الجرائم هي النساء والفتيات[٣].

٢- **الدافع تقني:** كلما زاد التطور التكنولوجي، كلما ادى ذلك الى ازياد الجرائم المعلوماتية بسبب سهولة الحصول على الصور والتسجيلات الصوتية والفيديوهات، مما يعمل المجرم المعلوماتي على استغلال هذا التطور التقني من اجل العمل على تزييف العميق للصور والفيديوهات والتسجيلات الصوتية، سواء كان بدافع المتعة او التعلم او ابراز مهارة لدية، مما ادى ذلك التطور الى ان تصبح هذه الجرائم اكثر وقوعاً من الجرائم التقليدية، لكونها من الجرائم التي ترتكب بسهولة وسرعة ومن دون ترك اي اثار وادله للجريمة، لذا نجد كلما تطور العالم الرقمي كلما انتشرت جرائم اصبحت ترتكب بطرق ذكية مثل جريمة التزييف العميق التي ظهرت مع تطور الذكاء الاصطناعي وتقنياته مما اساءه استخدام هذه التقنية من خلال تركيب صور لشخص ما على فيديو لشخص اخر وهو يقوم بحركات او يقول كلام غير واقع في الحقيقة أو العمل على فبركة الاصوات وتزيفها او تغيرها من اجل ابتزاز الشخص او التشهير به او

(١) د. محمد علي حسونة، الاستراتيجية الامنية في مجابهة الجرائم الالكترونية المستحدثة، دار النهضة العربية، مصر،٢٠٢٤، ص٥١.

(٢) د. أيمن عبد الله فكرى، جرائم نظم المعلومات (دراسة مقارنة)، دار الجامعة الجديدة للنشر، الاسكندرية، ٢٠٠٧، ص١١٥- ١١٦.

(٣) د. أميل جبار عاشور، فيصل غازي محمد، الاحكام الاجرائية للابتزاز الالكتروني للأطفال عبر مواقع التواصل الاجتماعي(دراسة مقارنة)، مجلد١، عدد٨، بحث منشور في مجلة ميسان للدراسات القانونية، كلية القانون، جامعة ميسان، ص٣٣٢.

تهديده، ومما يزيد صعوبة هذا الامر انه اصبح من الصعب التمييز بين الحقيقة والمزيف فيما ينشر على مواقع التواصل والاعلام(١).

٣- **الدافع السياسي:** يتم استخدام تقنية التزييف العميق من اجل دافع سياسي من خلال بث الخطابات الكراهية والتمييز والطائفية، او من خلال العمل على تزييف مقطع فيديو لشخصيات عامة مهمة في الدولة كرئيس الدولة أو احد وزرائها من اجل المساس بسمعته كما هو الحال عندما نشر فيدية للرئيس الفرنسي (ماكرون) وهو في لقاء صحفي ومن ثم قام بأفعال وحركات غير اخلاقية مع امرأه اثناء اللقاء الصحفي(٢)، او يتم العمل على تزييف مقطع فيديو لمرشح ما من طرف اخر من اجل التأثير على سمعته في العملية الانتخابية، كما يحصل الان في العديد من الدول، حيث تلجا حملة لطرف سياسي ما الى اساليب قذرة من اجل تشوية سمعة الطرف الخصم(٣).

- **دافع النقص في التشريعات الجنائية:** مع تطور العالم التكنولوجي وبقاء النصوص العقابية كما هي كانت من دون ان تواكب التطور الذي يشهده العالم الرقمي سبب رئيس في ازياد الجرائم المعلوماتية، مما دفع الافراد الى ارتكاب الجرائم المعلوماتية من دون اي خوف او تردد بحجه غياب النصوص العقابية المجرمة لهذه الافعال كما هو الحال في العراق ما زال لا يوجد لحد الان تشريع خاص بالجرائم الالكترونية، او انه يوجد تشريعات خاصة كما هو الحال في العديد من الدول التي سنت تشريعات جنائية خاصة بمكافحة الجرائم المعلوماتية، لكن هذه التشريعات تكون عقوباتها لا تتناسب مع الجرائم المرتكبة أو ان النصوص العقابية لا تشمل جميع هذه الافعال، كما هو الحال في جريمة التزييف العميق التي لم ينص على تجريمها بصورة ونصوص واضحة وصريحة في أي قانون لحد الان على الرغم لما لها من مخاطر واثار عميقة تمس الافراد والدول، كل هذه الاسباب ساعد المجرمين في ارتكاب الجرائم المعلوماتية من دون خوف او تردد بسبب القصور التشريعي وضعف العقوبة التي لا تتناسب او غير كافية لردع الجناة وغيرهم ممن تسول نفسهم لارتكاب مثل هذه الجريمة(٤).

---

(١) د. محمد عبيد الكعبي، الجرائم الناشئة عن الاستخدام غير المشروع لشبكة الانترنت، دار النهضة العربية، مصر،٢٠٠٩، ص١٠٢-١٠٣.

(٢) المقطع المزيف للرئيس الفرنسي ماكرون بتقنية التزييف العميق على تطبيق يوتيوب، على الرابط https://youtu.be،، تاريخ ووقت الزيارة١٥/١٠/٢٠٢٤، ٣:٠٠م.

(٣) د. علي مولود فاضل، سيف عدنان عباس، التزييف العميق، مرجع سابق، ص ٣٧.

(٤) روشن سردار محمد علي، المسؤولية الجنائية عن الجرائم الاخلاقية عبر مواقع التواصل الاجتماعي (دراسة مقارنة)، رسالة ماجستير، كلية القانون والعلوم السياسية، جامعة كركوك، العراق، ٢٠٢٢، ص٤٧.

الخاتمة

بعد ان انهينا البحث في موضوع التكييف القانوني لجريمة التزييف العميق، توصلنا الى مجموعة من النتائج والمقترحات، ونجملها بما يلي:

اولاً: النتائج

١- تعد جريمة التزييف العميق من الجرائم الحديثة التي انتجت من خلال التطور الذي شهدة الذكاء الاصطناعي وتقنياته المتطورة، والتي تعمل على انشاء محتوى مرئي أو صوتي مزيف يصعب تمييزه ومعرفته عن المحتوى الحقيقي.

٢- ما زالت اغلب التشريعات العربية ومنها الدول محل المقارنة مصر والامارات عن وضع نصوص تشريعية خاصة وواضحة تجرم التزييف العميق بنصوص صريحة، على الرغم من وجود تشريعات خاصة بالجرائم المعلوماتية لديها وهذا يعتبر قصور تشريعي في قوانينها، كما ان العراق ما زال من الدول المتأخرة التي لم توضع تشريع خاص بالجرائم المعلوماتية، وبالتالي سوف يتم الرجوع الى القوانين العقابية التقليدية من اجل مواجهة جريمة التزييف العميق والحد منها.

٣- في ظل غياب النصوص القانونية الصريحة التي تعاقب وتجرم اساءه استخدام تقنية التزييف العميق، ولكي لا يفلت الجاني من العقاب بحجة عدم وجود تشريع قانوني خاص، فأن الجهات القضائية المختصة بالتحقيق تبدأ في البحث عن التكييف القانوني الذي يتناسب مع هذا الفعل وتجريمه لكي لا يفلت الجناة من العقاب.

٤- ان لجريمة التزييف العديد من المخاطر والاثار الاجتماعية على الافراد من خلال انتهاك خصوصيتهم والتشهير بهم، كما ان لها مخاطر على المجتمعات والدول لما تشكل من تهديد للوضع الامني والسياسي والاقتصادي، حيث ان مخاطرها واضرارها التي تقع على المجني عليه تختلف باختلاف الدافع او الباعث الذي يهدف اليه بالجاني من ورا ارتكاب هذه الجريمة.

ثانياً: الاقتراحات

١- نقترح على المشرع العراقي على الاسراع بوضع تشريع قانوني خاص بمكافحة الجرائم المعلوماتية، كما يجب ان يلفت المشرع الى مخاطر الذكاء الاصطناعي وتقنياته المتطورة التي اصبحت اكثر

استخداماً في ارتكاب الجرائم، كما هو الحال في جريمة التزييف العميق التي يجب ان يكون هناك نص قانوني صريح يجرم اساءه استخدام هذه التقنية مع وضع عقوبات قوية ورادعة من أجل الحد منها ومواجهتها.

٢- نقترح ان تكون الاجهزة القضائية والجهات المختصة والرجال القائمين عليها ان يتمتعون بالخبرة والمعرفة والكفاءة في كيفية التعامل مع هذه الجرائم وكشفها ومعرفة مرتكبيها وضبط الادلة، لان هذه الجريمة تقع في عالم افتراضي.

٣- نرى ان تكون هناك زيادة في الوعي لدى المجتمعات من خلال اقامة حملات توعية في المدارس والجامعات واقامة الندوات، لكي يتم تعريف الافراد بمخاطر واضرار جريمة التزييف العميق.

المصادر

First_Legal Books

1. Dr. Mahmoud Zaki Zidan, Criminal Confrontation with the Illegal Use of Deepfake Technology (A Comparative Study), ١st ed., Dar Al Fikr Wal Qanun Publishing and Distribution, Egypt, ٢٠٢٥, p. ١٧. Ashraf Sayed Abu Al-Ela, Criminal Confrontation with the Risks of Deep Fake Technology and Its Impact on the Admissibility of Digital Evidence in Criminal Proofreading (A Comparative Analytical Study), ١st ed., Dar Al-Nahda Al-Arabiya, Egypt, ٢٠٢٤, p. ١٥.

2. Abu Al-Fadl Jamal Al-Din Muhammad ibn Makram ibn Manzur, Lisan Al-Arab, vol. ٩, ١st ed., Dar Sadir, Beirut, ١٩٩٨, p. ١٤٣
3. Abu Al-Hasan Ali ibn Ismail, known as Ibn Sida, Al-Muhkam wa Al-Muhit Al-A'zam, vol. ١١, ١st ed., Dar Al-Kutub Al-Ilmiyyah, Beirut, ٢٠٠٠, p. ٩٣.
4. Akram Karim Khadir, In-Depth Studies in the Philosophy of Criminal Law, Academic Center for Publishing, Alexandria, Egypt, ٢٠٢٣, pp. ١٢٢-١٢١.
5. Muhammad Ali Abu Ali, Criminal Liability for Artificial Intelligence Damages, ١st ed., Dar Al-Nahda Al-Arabiya, Egypt, ٢٠٢٤, p. ٢٢.
6. Dr. Ashraf Sayed Abu Al-Ela, Criminal Confrontation with the Risks of Deep Fake Technology and Its Impact on the Admissibility of Digital Evidence in Criminal Proofreading (A Comparative Analytical Study), ١st ed., Dar Al-Nahda Al-Arabiya, Egypt, ٢٠٢٤, pp. ٢١-٢٠.

7. Dr. Basem Muhammad Fadel, Legal Challenges of Deep Fake Technology, A Comparative Analytical Study, ١st ed., Dar Al-Fikr Al-Jami'i, Egypt, ٢٠٢٥, p. ٤٥.
8. Dr. Ali Mawloud Fadel, Saif Adnan Abbas, Deep Fake: The Language of Artificial Intelligence in Media Cyberwars, ١st ed., Dar Amjad for Publishing and Distribution, Jordan, ٢٠٢٢, p. ٣٤.
9. Dr. Baraa Munther Kamal, Dr. Nouris Rashid Taha, Criminal Confrontation with Electronic Blackmail, ١st ed., Dar Al-Masala, Baghdad, Iraq, ٢٠٢٤, p. ٤٩.
10. Dr. Muhammad Ali Hassouna, Security Strategy for Confronting Emerging Cybercrimes, Dar Al Nahda Al Arabiya, Egypt, ٢٠٢٤, p. ٥١.
11. Dr. Ayman Abdullah Fikry, Information Systems Crimes (A Comparative Study), Dar Al Jamiaa Al Jadida Publishing House, Alexandria, ٢٠٠٧, pp. ١١
12. Dr. Muhammad Ubaid Al Kaabi, Crimes Arising from the Illegal Use of the Internet, Dar Al Nahda Al Arabiya, Egypt, ٢٠٠٩, pp. .١٠٣-١٠٢

second_ University theses

1. Mayada Muhammad Ahmad, Legal Conditioning of Facts in Criminal Cases (Comparative Study), PhD Thesis, College of Law, University of Mosul, Iraq, 2020, p. 12.
2. Muhammad Ibrahim Al-Alili, Procedural Confrontation of Cybercrimes (A Comparative Study), PhD Thesis, College of Law, University of Sharjah, United Arab Emirates, 2023, p. 19.
3. Ghadeer Majadeb Al-Ruwaili, Criminal Liability for Misuse of Deepfake Technology (A Comparative Study), Master's Thesis, College of Criminal Justice, Naif Arab University for Security Sciences, Saudi Arabia, 2023, p. 16.
4. Rowan Yaqoub Saeed Al-Zayan, Electronic Blackmail in Palestinian Legislation (A Comparative Study of Islamic Jurisprudence), Master's Thesis, College of Sharia and Law, Islamic University of Gaza, Palestine, 2023, pp. 19-20. Duaa Suleiman Abdul Qader Al-Tamimi, The Crime of Electronic Blackmail (A Comparative Study), Master's Thesis, Faculty of Law, Al-Quds University, Abu Dis, Jerusalem, Palestine, 2019, pp. 13-18.
5. Baqir Ghazi Hanoun Al-Daraji, Criminal Liability Arising from Electronic Blackmail (A Comparative Study), Master's Thesis, Faculty of Law, University of Basra, Iraq, 2020, pp. 69-73.
6. Roshan Sardar Muhammad Ali, Criminal Liability for Moral Crimes Through Social Media (A Comparative Study), Master's Thesis, Faculty of Law and Political Science, University of Kirkuk, Iraq, 2022, p. 47.

Third – Legislation

1. Article (202) of the Egyptian Penal Code No. (58) of 1937, as amended.
2. Egyptian Anti-Information Technology Crimes Law No. (175) of 2018.
3. Article (204) of the UAE Penal Code No. (3) of 1987, as amended.
4. UAE Anti-Rumors and Cybercrime Law No. (34) of 2021, as amended.
5. Articles (9, 99, 280, 284) of the Iraqi Penal Code No. (111) of 1969, as amended.
6. Iraqi Anti-Cybercrime Draft Law of 2019.
7. Articles (308, 327) of the Egyptian Penal Code No. (58) of 1973, as amended.
8. Articles (25, 26) of the Egyptian Anti-Technical Crimes Law No. (175) of 2018.
9. Article (42/Paragraph 1) of the UAE Anti-Rumors and Cybercrimes Law No. (34) of 2021, as amended.
10. Text of Article (327) of the Egyptian Penal Code No. (58) of 1937, as amended.
11. Text of Article (42/Paragraph 2) of the Anti-Rumors and Cybercrimes Law No. (34) of 2021, as amended.
12. Articles (430-432) of the Iraqi Penal Code No. (111) of 1969, as amended.
13. Article (6) of the Iraqi Anti-Cybercrimes Draft Law of 2019.

Fourth – Legal research and article

1. Dr. Muhannad Hamid Obaid, "The Impact of Deep Fake in Digital Media on the Credibility of Television News Sources," a study published in the Journal of Media Studies and Research (M.S.A.R.), Volume 3, Issue 10, 2023, p. 265.
2. Dr. Al-Assad Saleh Al-Assad, "Ethical Concerns Over the Negative Uses of Artificial Intelligence Technologies - Deep Fake Technology as a Model," a study published in the Journal of Media Studies, Volume 6, Issue 2, 2022, p. 376.
3. See Al Jazeera.net, a news website affiliated with Al Jazeera Channel, at the link: https://www.aljazeera.net, date and time of visit: 10/23/2024, 10:00 PM.
4. Dr. Abdul Nasser Wannous, Lujain Khaddour, Some Applications of Deepfake Technology and Its Use in Contemporary Marketing and Promotion, a study published in the Damascus University Journal of Engineering Sciences, Volume 39, Issue 2, 2023, p. 10. Reda Ibrahim Abdullah Al-Bayoumi, "Legal Protection from the Risks of Deep Forgery Applications in Islamic Jurisprudence and Positive Law (A Comparative Analytical Study)," Special Issue, Eighth International Scientific Conference - Technology and Law, published in the Journal of the Spirit of Laws, Volume 35, Issue 102, 2023, pp. 843-844.

5. Muhammad Mustafa Salah Abdel Hamid, "Digital Forgery and Its Impact on the Admissibility of Digital Evidence in Criminal Cases (A Comparative Jurisprudential Study)," Research published in the Journal of Sharia and Law, Faculty of Sharia and Law, Al-Azhar University, Cairo, Issue 40, 2022, pp. 856-857.
6. Muhammad Ali Salem and Hassoun Obaid Hajij, "Cybercrime," Research published in the Journal of the University of Babylon for Humanities, Volume 14, Issue 2, 2007, p. 90. Rana Hikmat Abbas, "Electronic Blackmail," a study published in the Lark Journal of Philosophy, Linguistics, and Social Sciences, Volume 1, Issue 44, College of Arts, Department of Sociology, University of Wasit, Iraq, 2022, p. 472.
7. Dr. Amil Jabbar Ashour, Faisal Ghazi Muhammad, "Procedural Provisions for Electronic Blackmail of Children via Social Media (A Comparative Study)," Volume 1, Issue 8, a study published in the Maysan Journal of Legal Studies, College of Law, University of Maysan, p. 332.
8. Muayyad Jabbar Muhammad, Judicial Adaptation of Penal Rules: Their Application in the Absence of Criminal Legislation for New Crimes in Iraq as a Model, a study published in the Maysan Journal of Comparative Legal Studies, College of Law, University of Maysan, Issue 10, Volume 1, 2024, p. 609.
9. Muhammad Sattar Jabbar, The Administration's Obligation to Prevent Rumors Harmful to the Operation of Public Utilities, a study published in the Maysan Journal of Comparative Legal Studies, College of Law, University of Maysan, Issue 9, Volume 1, 2024, pp. 427-428.
10. The fake clip of French President Macron using deepfake technology on YouTube, at the link https://youtu.be, date and time of visit: October 15, 2024, 3:00 PM.

Fifth – Judicial decisions

1. Decision of the Babylon Court of Appeal, in its capacity as Court of Cassation, No. (926/T/C/2023), dated May 14, 2023 (published).
2. Decision No. (3758/Criminal Panel/2019), dated March 17, 2019 (unpublished), quoted from the reference, Dr. Baraa Munther Kamal, Dr. Nouris Rashid Taha, Criminal Response, op. cit., p. 55.