https://doi.org/10.61353/ma.0210133

الحماية الجنائية من المحتويات الاصطناعية غير التوافقية – دراسة تحليلية مقارنة

أ.م.د. ضياء مسلم عبد الامير
كلية القانون/ جامعة الكوفة
dhiaam.alghaibi@uokufa.edu.iq

تاريخ استلام البحث ٤/١٧ /٢٠٢٥ تاريخ ارجاع البحث ٢٠٢٥/٥/١ تاريخ قبول البحث ٢٠٢٥/٥/١٨

إن مواجهة التحديات التي تفرضها التقنيات الحديثة على المنظومة القانونية باتت ضرورة ملحة لضمان سيادة القانون في الفضاء الرقمي تمامًا كما هو في الواقع المادي, إذ إن هناك جهودًا دولية متقدمة لوضع إطار قانوني رادع للاستخدام السيء للتكنولوجيا وخصوصا أدوات الذكاء الاصطناعي المتقدمة، بينما ما زالت بعض الدول، ومنها العراق، في طور إدراك أبعاد المشكلة . ومع ذلك، فإن الفرصة متاحة للاستفادة من تجارب الدول وخاصة القانون الفرنسي والقانون الاماراتي ، وتطويعها لاستنباط الحلول التشريعية المناسبة للمشرع العراقي، إن هذا البحث يؤكد على أهمية إيجاد توازن تشريعي يضمن حماية فعالة للأفراد والمجتمع من المحتويات الاصطناعية غير التوافقية، بدون إهدار لضمانات حرية التعبير عبر صياغة محددة للأفعال المجرّمة واستثناء الحالات المشروعة بوضوح، مع إقرار جزاءات مناسبة. ولا شك أن المضي قدمًا في مقترحات هذا البحث وخاصة النصوص القانونية المقترحة للمشرع العراقي سيكون عاملاً حاسمًا في تقليل إساءة استخدام تقنيات الذكاء الاصطناعي، وردع كل من يفكر في تحويلها إلى أداة للاعتداء على كرامة الافراد أو أمن المجتمع. وبينما تستمر التكنولوجيا في التطور بوتيرة متسارعة، يظل الواجب على القانون أن يتطور بخطى ثابتة لضمان أن تبقى الحقوق والحريات مصونة، وأن يُساءل كل من يتجاوز الحدود تحت ستار التقنيات الحديثة، تحقيقًا للعدالة وحمايةً للمجتمع.

الكلمات المفتاحية: التشريع الجنائي, المحتويات الاصطناعية غير التوافقية, الذكاء الاصطناعي, حماية الحقوق والحريات, العقوبات , التدابير الاحترازية.

Confronting the challenges posed by modern technologies to the legal system has become an urgent necessity to ensure the rule of law in the digital space just as it is in the physical world. While there are advanced international efforts to establish a robust legal framework to deter the misuse of technology—particularly sophisticated artificial intelligence tools—some countries, including Iraq, are still in the early stages of understanding the full scope of the issue. Nevertheless, there remains a valuable opportunity to benefit from the experiences of other nations, especially the French and Emirati legal systems, and to adapt these experiences in formulating appropriate legislative solutions tailored to the Iraqi context.This study emphasizes the importance of achieving a legislative balance that provides effective protection for individuals and society against harmful synthetic content, without compromising the guarantees of freedom of expression. This can be achieved through clear definitions of criminalized acts, explicitly excluding legitimate cases, and by introducing proportionate penalties. Undoubtedly, advancing the proposals of this research—particularly the suggested legal texts for the Iraqi legislator—will play a pivotal role in minimizing the misuse of AI technologies and deterring anyone who seeks to exploit them as tools for violating human dignity or societal security. As technology continues to evolve rapidly, the law must progress steadily to ensure that rights and freedoms remain protected, and that anyone who oversteps the boundaries under the guise of modern technology is held accountable, in pursuit of justice and the protection of society..

Keywords: Criminal Legislation, Non-consensual Synthetic Content, Artificial Intelligence, Protection of Rights and Freedoms, Sanctions, Preventive Measures.

المقدّمة

شهدت السنوات الأخيرة تناميا مذهلاً في قدرة التقنيات الرقمية على توليد محتوى اصطناعي يحاكي الواقع بشكل يخادع البصر والسمع. ويطلَق على هذا المحتوى المصطنع بالذكاء الاصطناعي تسمية المحتويات الاصطناعية غير التوافقية ,وتعني هذه العبارة كل صورة، أو فيديو أو تسجيل صوتي يتم توليده أو تعديل مضمونه بواسطة خوارزميات الذكاء الاصطناعي بحيث يظهر شخصا حقيقيا يقوم بأفعال أو أقوال لم تصدر عنه فعليا، وذلك دون موافقته أو رضاه. إن موضوع هذه الدراسة هو البحث في سبل الحماية الجنائية للأفراد والمجتمع من أخطار هذا المحتوى الاصطناعي غير التوافقي، عبر دراسة مقارنة بين القانون الفرنسي والإماراتي والعراقي، للتعرف عل كل منها لهذا التحدي التقني الحديث.

أهمية البحث: تكمن أهمية البحث في خطورة المحتويات الاصطناعية المزيفة على عدد من المصالح المحمية قانوناً؛ فهي باتت تُهدد الأمن الرقمي والثقة العامة في المعلومات المنشورة عبر الفضاء تسبب في انتهاك الخصوصية وتشويه سمعة الأفراد على نطاق واسع وبصورة غير مسبوقة حديثة أن تقنية التزييف تَستغل بشكل متزايد ضد النساء، إذ وجد أن نحو ٩٦٪ من مقاطع الفيديو المزيفة عميقًا على الإنترنت ذات طابع إباحي تستهدف بالأساس نساء مشهورات بدون موافقتهن، مما يشكّل انتهاكًا فجا لخصوصيتهن وكرامتهن. وبالموازاة، برزت استخدامات خبيثة أخرى لهذه التقنيات كعمليات الاحتيال الإلكتروني وانتحال الهوية لنشر معلومات مضللة تهدد الأمن العام.

مشكلة البحث: تتضمن في قصور الأطر القانونية التقليدية عن مواجهة هذه الظاهرة المستجدة، وحاجة التشريعات الجنائية إلى تطوير أدواتها لملاحقة ومعاقبة من ينتج أو ينشر المحتويات الاصطناعية غير التوافقية. وتزداد المشكلة تعقيدًا عند النظر إليها في إطار مقارن؛ إذ تتفاوت استجابات الدول: فبينما أدخل المشرع الفرنسي نصوصا صريحة لتجريم هذا الفعل، يتميز القانون الإماراتي بأحكام عامة ومرنة تَستخدم لملاحقة مرتكبي هذه الجرائم حين لا يزال القانون العراقي يفتقر لنصوص صريحة في هذا المجال ويعتمد على تكييفات تقليدية قد تصطدم بمبدأ الشرعية الجنائية. لذا فإن الغرض هو تبيان مواطن القوة والضعف في نهج كل نظام قانوني، وصولًا إلى اقتراح توصيات لتطوير التشريع العراقي في ضوء التجارب المقارنة.

أهداف البحث: يسعى البحث إلى تأصيل المفهوم الخاص بالمحتويات الاصطناعية غير التوافقية مع تحليل المخاطر القانونية والاجتماعية المترتبة على انتشار هذا المحتويات في فرنسا والإمارات والعراق المتعلقة بمكافحة هذه الظاهرة، من حيث التجريم والإجراءات، وبيان أوجه الاتفاق والاختلاف بينها, فضلاً عن استخلاص الدروس التشريعية وتقديم مقترحات محددة لتعزيز الحماية الجنائية في العراق

نطاق البحث: يتحدد البحث من ضمن نطاق القانون الجنائي الموضوعي والإجرائي في كل من فرنسا والإمارات والعراق, مع التركيز على إعطاء مقترحات قانونية للمشرع العراقي بالإفادة من الدول محل البحث.

منهجية البحث: يعتمد البحث المنهج الوصفي التحليلي المقارن؛ إذ سيتم وصف ظاهرة المحتوى الاصطناعي غير التوافقي وتقنياتها، ثم تحليل الإطار القانوني الجنائي في النظم محل الدراسة والتطبيقات القضائية المتاحة.

هيكلية البحث: ينتظم البحث في مبحثين رئيسين يتفرع كل منهما على مطالب وفروع، على النحو الآتي:

- المبحث الأول: الإطار المفاهيمي للمحتويات الاصطناعية غير التوافقية. ويشمل بيان ماهية هذه المحتويات عن طريق تعريفها وشرح خصائصها ثم مناقشة المخاطر المترتبة عليها سواء فيما يتعلق بأمن الفضاء الإلكتروني والثقة العامة، أو بحقوق الأفراد في الخصوصية والسمعة.
- المبحث الثاني: الإطار القانوني للحماية الجنائية من المحتويات الاصطناعية غير التوافقية. ويشمل شقين أساسين: الشق الموضوعي للحماية ، ثم الشق الإجرائي للحماية عبر بحث وسائل إثبات هذه الجرائم وتحدياتها، ودور الأجهزة القضائية والتنظيمية في ملاحقة الجناة والتعاون الدولي.

المبحث الأول: الإطار المفاهيمي للمحتويات الاصطناعية غير التوافقية

يسعى هذا المبحث إلى بناء فهم نظري وتقني واضح لظاهرة المحتويات الاصطناعية غير التوافقية من حيث تعريفها وماهيتها، ونشأة هذه التقنية وتطورها التاريخي، ثم بيان أهم المخاطر والآثار السلبية الناجمة عنها. ويقسم المبحث على مطلبين: يتناول الأول ماهية المحتويات الاصطناعية غير التوافقية (التعريف والنشأة)، ويتناول الثاني أبرز المخاطر المترتبة على انتشارها.

المطلب الأول: ماهية المحتويات الاصطناعية غير التوافقية

سنتناول هذا المطلب في فرعين, الأول تعريف المحتويات الاصطناعية غير التوافقية , ونشأة وتطور المحتويات الاصطناعية غير التوافقية في الفرع الثاني

الفرع الأول: تعريف المحتويات الاصطناعية غير التوافقية

يقصد بالمحتويات الاصطناعية غير التوافقية ذلك المحتوى الرقمي الزائف الذي يتم إنشاؤه بواسطة تقنيات الذكاء الاصطناعي بطريقة تحاكي محتوى حقيقي يتعلق بشخص معين دون أن يصدر عنه فعليا أو أذن به. بعبارة أخرى، هو كل صورة أو مقطع فيديو أو مقطع صوتي متلاعب به رقميا ليظهر شخصا حقيقيا (سواء كان من المشاهير أم الأفراد العاديين) وهو يقول أقوالًا أو يرتكب أفعالًا لم تحدث في الحقيقة. ويشمل ذلك تبديل وجه شخص بآخر في مقاطع الفيديو ، أو توليد صورة شخص بوضعيات لم يلتقطها في الواقع، وذلك باستخدام خوارزميات[١]. وفيما يخص التعبير الدارج "التزييف العميق Deepfake" فانه يشير الى هذه الظاهرة لكونها ناتجة عن تقنيات التعلم العميق ولأنها تنطوي على تزوير وخداع متقن. في السياق الفرنسي، كما يشار إلى هذه المحتويات بمصطلح "Hypertrucage" أي "التزوير الفائق"[٢].

الا إن وصف المحتويات الاصطناعية غير التوافقية هو اكثر من ذلك , اذ ان "غير التوافقية" يلحق بالمحتويات الاصطناعية للإشارة إلى أنها بدون رضا الأشخاص الذين تتعلق بهم هذه المحتويات. وقد برز هذا الوصف تحديدا في سياق الصور الحميمية أو الإباحية المنتجة ذكاء اصطناعيا دون موافقة أصحابها، حيث

استخدم مصطلح "الصور الحميمية غير التوافقية" للتفريق بينها وبين الصور الحقيقية المسربة بدون إذن. وبشكل عام، يصبح المحتوى الاصطناعي "غير توافقي" متى ما تضمن انتهاكًا لحقوق الشخص المنتحلة هويته أو صورته دون إذنه، سواء كان محتوى إباحيا أو تشهيريا أو تضليليا. وتعكس عدم التوافقية هنا عنصرا جوهريا في تجريم إذ أن محور الاعتداء يكمن في افتقار الفعل لموافقة المعني بالأمر، مما يجعله انتهاكًا لحقه في صورته وصوته وسمعته[٣].

وتجدر الإشارة إلى أن المحتويات الاصطناعية قد لا تكون جميعها غير مشروعة أو ضارة بالضرورة؛ فالتزييف العميق يمكن استخدامه في مجالات مشروعة مثل صناعة السينما (كإعادة إنشاء وجوه الممثلين في مشاهد معينة)، أو في تطبيقات تعليمية وترفيهية، أو حتى لأغراض سخرية سياسية من ضمن حدود حرية التعبير[٤]. بيد أن وصف "غير التوافقية" يضيق نطاق البحث على الاستخدامات الخاصة بها لهذا المحتوى، حيث يصبح وسيلة للاعتداء على الآخرين أو خداع الجمهور. وعليه تنصب الاهتمامات القانونية على التزييف العميق الضار الذي يستهدف الإساءة إلى شخص معين أو إلى المصلحة العامة دون رضا الأطراف المتضررة.

لقد تناولت بعض القوانين الحديثة مفهوم المحتوى الاصطناعي الزائف بالتعريف. فعلى سبيل المثال، نص القانون الفرنسي الصادر في ٢١ أيار/مايو ٢٠٢٤ (المعروف بقانون تأمين وتنظيم الفضاء الرقمي SREN) على تعديل المادة ٢٢٦-٨ من قانون العقوبات ليشمل تجريم نشر أي محتوى مرئي أو سمعي مولّد بالمعالجة الخوارزمية يمثل صورة أو كلام شخص دون موافقته، ما لم يكن واضحا أو مصرحا بأنه مصطنع. يتضح من هذا التعريف التشريعي أن المشرع الفرنسي يعتبر عدم الإفصاح عن كون المحتوى مزيفًا قرينة على نية الخداع والمعاقبة. أما إذا كان المحتوى الإصطناعي واضحا للجمهور أنه غير حقيقي أو تم التنويه إلى زيفه بشكل صريح، فإنه يخرج من نطاقه , يبرز ذلك حرص القانون على موازنة حرية الابتكار والتعبير مع ضرورة حماية الحقوق؛ فالأصل في استخدام تقنيات الذكاء الاصطناعي هو الإباحة ما لم تستغل للإضرار بالغير[٥].

وخلاصة القول، يمكن تأطير تعريف المحتويات الاصطناعية غير التوافقية بأنها: "كل صورة، أو فيديو، أو تسجيل صوتي أو أي مخرجات رقمية أخرى يتم توليدها أو تعديلها بواسطة الذكاء الاصطناعي بحيث تنسب لشخص طبيعي أقوالاً أو أفعالاً لم يأذن بها ولم تقع منه حقيقة، وكان من شأنها أن تسبب له ضررا معنويا أو ماديا". هذا التعريف يركز على عناصر الاصطناع التقني (باستخدام AI أو وسائل رقمية حديثة) وانتحال الهوية أو الفعل العائد لشخص آخر، وغياب رضا الشخص المنتحلة هويته، فضلاً عن احتمال وقوع ضرر كنتيجة لذلك الانتحال أو الخداع. هذه العناصر مجتمعة تميز المحتوى الاصطناعي غير التوافقي عن غيره من صور التزوير، وتشكل الأساس لتجريمه كما سيأتي في المباحث اللاحقة.

الفرع الثاني: نشأة وتطور المحتويات الاصطناعية غير التوافقية

لم تظهر تقنية التزييف العميق دفعة واحدة، بل جاءت ثمرة تطورات متسارعة في ميدان الذكاء الاصطناعي ومعالجة الصور خلال العقد الأخير. يمكن تتبع النشأة التاريخية للمحتويات الاصطناعية غير التوافقية إلى عام ٢٠١٧ عندما قام مستخدم على منصة "Reddit" يحمل الاسم المستعار "deepfakes" بنشر أولى مقاطع الفيديو المفبركة باستخدام خوارزميات التعلم العميق. وقد أثارت تلك المقاطع التي كانت عبارة عن مشاهد إباحية جرى تركيب وجوه ممثلات مشهورات عليها , ضجة كبيرة كونها أظهرت مدى القدرة على تزييف الواقع رقميا بخداع شديد الإتقان [٦]. وسرعان ما انتشرت أساليب إنشاء التزييف العميق عبر مجتمع الإنترنت، إذ توافرت برمجيات مفتوحة المصدر لتبديل الوجوه واستخدام شبكات "GAN" لتوليد صور أشخاص غير حقيقية أو دمج ملامح شخصين[٧]. وبحلول عام ٢٠١٩، رصدت إحدى الدراسات وجود أكثر من ١٥,٠٠٠ فيديو تزييف عميق منشور على الإنترنت، ٩٦٪ منها ذو طبيعة إباحية تستهدف بالأساس نساء دون موافقتهن وهذا يدل على تضاعف حجم المحتوى المزيف في غضون أشهر قليلة وتركزه في الاستخدامات الأكثر انتهاكاً للخصوصية (المواد الإباحية غير التوافقية)[٨].

ترافق هذا الانتشار مع تحسن نوعي كبير في دقة وجودة التزييف العميق بفضل تطور خوارزميات التعلم العميق وقدرات المعالجة. فبعد أن كانت المقاطع المزيفة المبكرة تعاني من عيوب مرئية يمكن كشفها بسهولة نسبيا (مثل وميض في ملامح الوجه أو عدم تزامن مثالي لحركة الشفاه)، أصبحت الأجيال الأحدث قادرة على إنتاج فيديوهات وصور بالغة الواقعية[٩].

كما انه لم يعد إنتاج "Deepfake" حكرا على الخبراء. فاليوم توجد تطبيقات للهواتف الذكية تتيح تبديل الوجوه في الصور والفيديوهات خلال دقائق وبجهد قليل. وإن التطور التقني المتواصل يطرح تحديا مستمرا، فكلما ظهرت أساليب لكشف يأتي الذكاء الاصطناعي على تحسين خوارزمياته لتفادي الكشف. وقد دخلت في هذا السباق أيضا بعض الجهات الرسمية والتجارية؛ فمثلاً أعلنت شركات تقنية قدرتها على تحليل الأنماط الرقمية الخفية أو ما يعرف بـ"بصمة الذكاء الاصطناعي" بينما بدأت منصات التواصل الاجتماعي الكبرى في حظر ومراقبة المحتوى المزيف، فمثلا شركة (META) وضعت سياسة وتقنيات للمطابقة وحذف المزيف تلقائيا من منصاتها. وبالرغم من ذلك، يبقى من الصعب مواكبة هذا السباق بشكل كامل[١٠].

على الصعيد المفاهيمي، أثار ظهور التزييف العميق نقاشات حول مدى كفاية المفاهيم القانونية التقليدية لمواجهة فبعضهم عدها امتدادا لجرائم انتحال الهوية، أو التشهير ولكن بوسائل تقنية مستحدثة، في حين رأى آخرون أنها تشكل نوعا خاصا[١١]. وقد واجه المشرعون حول العالم هذه الظاهرة ؛ في حين تأخرت التشريعات في بعض الدول، سارع المشرع الفرنسي , كما سيأتي بيانه , إلى سن تعديل قانوني صريح بشأن المحتويات المصطنعة. أما على المستوى الدولي جرى إدراج هذه القضية من ضمن مبادرات أوسع تتعلق بتنظيم

https://doi.org/10.61353/ma.0210133

الذكاء الاصطناعي الأوروبي AI Act الذي يناقش وضع التزامات على مخرجات الذكاء الاصطناعي الخطرة، والجرائم الإلكترونية عموما[١٢].

وخلال هذا التطور التاريخي، برز صنف خاص ذو أهمية من المحتويات الاصطناعية غير التوافقية هو المحتوى الإباحي المزيف الذي يستغل أشخاصا (غالبا نساء) بوضعيات فاضحة دون علمهم. هذا الصنف ذو خطورة كبيرة اذ يعدّ انتهاكا للخصوصية والكرامة الإنسانية. وقد تفاعلت المنظمات الدولية والنسوية مطالبةً بتجريم خاص سواء أكانت الصور حقيقية، أم مزيفة. واستجابة لذلك اتجهت دول مثل فرنسا إلى استحداث نصوص تُجرم "المحتوى الجنسي غير التوافقي" صراحةً، كما سيأتي بيانه.

يتضح مما سبق أن المحتويات الاصطناعية غير التوافقية هي نتاج تطور تقني حديث العهد نسبياً (خلال أقل من عقد)، لكنها شهدت انتشارا واسعا ونموا مطّردا في فترة وجيزة. وقد تراوحت استخداماتها بين أهداف ترفيهية أو فنية مشروعة وبين أعمال تخريبية وإجرامية خطيرة. وبذلك نشأ واقع جديد فرض على القانون ضرورة التطور لملاحقة إساءة استخدام هذه التقنية. في المطلب التالي سيتم التركيز على أهم المخاطر والتهديدات الناجمة عن المحتويات الاصطناعية غير التوافقية، تمهيدًا لفهم دوافع التجريم والحماية الجنائية التي ستناقش في المبحث الثاني.

المطلب الثاني: المخاطر الناشئة عن المحتويات الاصطناعية غير التوافقية

مع الانتشار المتزايد لتقنيات التزييف الاصطناعي، برزت جملة من المخاطر الجسيمة التي تؤثر على مستويات عدة؛ منها ما يهدد أمن المعلومات والثقة العامة في الفضاء الإلكتروني، ومنها ما ينال من حقوق الأفراد في الخصوصية والسمعة الحسنة بل وقد يسبب أضرارا نفسية واجتماعية بالغة. سنقسم دراسة المخاطر على فرعين أساسيين: يتناول الأول تأثير المحتويات الاصطناعية غير التوافقية على الأمن الرقمي والثقة المجتمعية، ويتناول الثاني أثرها على الحقوق الشخصية للأفراد كالخصوصية والسمعة.

الفرع الأول: تهديد الأمن الرقمي والثقة العامة في الفضاء الإلكتروني

أحدثت تقنية التزييف العميق هزة في موثوقية المعلومات الرقمية إلى حد دفع بعضهم للقول إننا دخلنا عصر "ما بعد الحقيقة" إذ لم يعد بالإمكان الجزم بصحة ما نراه أو نسمعه عبر الإنترنت. ويمكن إجمال أهم أوجه تهديد المحتويات الاصطناعية غير التوافقية للأمن الرقمي والثقة العامة بالنقاط الآتية:

اولا: الاحتيال الإلكتروني وانتحال الهوية (Digital Fraud & Identity Theft): أصبحت المقاطع والصور المزيفة أداة جديدة في يد المحتالين لارتكاب جرائم النصب والاحتيال عبر الإنترنت. فباستخدام فيديو أو صوت مولّد بالذكاء الاصطناعي، يمكن للجاني انتحال شخصية مسؤول أو مدير شركة وإصدار تعليمات أو طلبات كاذبة توقع الضحايا في فخاخ مالية. وقد شهدت عدة دول حوادث فعلية من هذا النوع؛ منها على سبيل المثال عملية احتيال دولية في دبي عام ٢٠٢٠ تورط فيها مجموعة من الأشخاص ضمن عصابة استخدمت الذكاء الاصطناعي لسرقة ٣٦ مليون دولار عبر انتحال صوت

وصورة مسؤولين[١٣]. كذلك وقع مسؤول في شركة بريطانية ضحية مكالمة صوتية مزيفة يعتقد أنها بصوت المدير التنفيذي لشركته يطلب منه تحويل أموال، مما تسبب بخسارة نحو ٢٤٣ ألف دولار[١٤]. هذه الأمثلة تبين كيف يمكن للتزييف العميق اختراق أنظمة الحماية القائمة على التحقق الصوتي، أو المرئي وخداع حتى الأشخاص الحذرين، مهددا بذلك أمن المعاملات الإلكترونية وثقة الأفراد في هوية المتصلين رقميا, وهكذا بات على الأنظمة الأمنية والتجارية أن تأخذ بالحسبان هذا الجيل الجديد من الخدع الرقمية.

ثانيا: نشر الأخبار الكاذبة وتضليل الرأي العام (Misinformation & Fake News): تمثل المحتويات الاصطناعية غير التوافقية أداة فعالة في يد مروجي الشائعات وحملات التضليل الإعلامي، إذ يمكن عبرها صنع أحداث وهمية وإسناد تصريحات مفبركة لمسؤولين أو شخصيات عامة بغرض تضليل الجمهور. خطورة التزييف العميق هنا أنه يمنح الشائعة قالبا بصريا/سمعيا ملموسا يزيد من قابلية تصديقها وانتشارها. فعلى سبيل المثال، قد يتمكن قراصنة من اختراق بث تلفزيوني لبث خبر مزيف عبر مذيع توليدي يقدم معلومات كاذبة عن احداث سياسية، مما يثير بلبلة قبل كشف الحقيقة. وبالمثل يمكن تخيل تداعيات مقطع مزيف يظهر رئيس دولة يعلن قرارا خطيرا (كإعلان حالة حرب، أو فرض إجراءات طوارئ) وما يمكن أن يسببه من فوضى واضطراب اجتماعي قبل اكتشاف زيفه. إن الثقة العامة في وسائل الإعلام والمحتوى الرقمي أصبحت على المحك؛ فالجمهور بات حائرا بين تصديق ما يراه أو التشكيك حتى في الحقائق الصحيحة خشية أن تكون مزيفة، وهذا بحد ذاته أثر ضار يعرفه الباحثون بـ"أثر الكذاب" (liar's dividend) حيث يمكن للمسؤولين الفاسدين مثلاً إنكار أي أدلة ضدهم بزعم أنها مزيفة عميقاً. وقد أكد مجلس الأمن السيبراني في الإمارات في تحذير رسمي حديث أن تقنية التزييف العميق تثير مخاوف جدية لنشر المعلومات المضللة بما يؤدي لزعزعة الثقة بالأخبار والمحتوى الرقمي[١٥]. وعليه، يشكل انتشار هذه التقنية تحديا لمصداقية البيئة المعلوماتية برمتها، مما يستوجب تعزيز جهود التوعية الرقمية وتطوير تقنيات مضادة تكشف المحتوى الزائف حمايةً للصالح العام.

ثالثا: تهديد الأمن الوطني والسلم الأهلي: بالرغم من أن الأمثلة السابقة تبين جانبا من المخاطر على الأمن العام، إلا أن الأمر يستحق إفراد نقطة خاصة لتأثير التزييف العميق على الأمن الوطني للدول. إذ يمكن استخدامه كأداة في الحرب النفسية والسيبرانية بين الدول والجماعات المتنازعة. تخيل سيناريو يقوم فيه طرف معاد بفبركة خطاب مرئي لقائد عسكري يدعو جنوده للاستسلام، أو مقطع مزيف لمسؤول أمني يعترف بأسرار حساسة. مثل هذه العمليات قد تفقد القوات أو المواطنين ثقتهم بقيادتهم أو تحدث ارتباكاً في صفوف الجبهة الداخلية. وقد بدأت بوادر استخدام التزييف العميق في هذا المجال فعلاً، إذ تحدثت تقارير عن محاولات لبث رسائل مزيفة خلال نزاعات مسلحة بغرض إضعاف الروح المعنوية أو تسويغ اعتداءات. وعليه، ينظر الخبراء إلى التزييف العميق كواحد من التهديدات الصاعدة للأمن القومي

الذي قد يستغل ثغرات القانون الدولي وعدم جاهزية العديد من الدول تكنولوجيا لمواجهته. كذلك قد يؤدي نشر فيديوهات مفبركة ذات محتوى طائفي أو تحريضي منسوبة زورا إلى شخصيات دينية أو سياسية إلى إثارة الفتن الأهلية واضطراب السلم المجتمعي، خاصة في دول متعددة المكونات الاجتماعية. ولعل هذا الجانب من أخطر ما يمكن أن ينجم عن إساءة استخدام التزييف العميق، إذ يُحول التقنية من مجرد خدع فردية إلى سلاح استراتيجي لزعزعة استقرار المجتمعات[١٦].

رابعا: إضعاف الثقة بالبنية الرقمية والقضاء (Eroding Trust in Digital Systems & Justice): إذا ما انتشرت حالات نجاح التزييف العميق في خداع الناس والمؤسسات، فإن أثر ذلك سيمتد إلى تآكل الثقة في البنية التحتية الرقمية ككل. على سبيل المثال، قد يتراجع الاعتماد على وسائل التواصل الإلكتروني الرسمية لإيصال المعلومات خشية التزوير، أو قد يعاد النظر في موثوقية أنظمة التحقق بالتعرف على الوجه أو الصوت في المعاملات الأمنية والمالية. وبالنسبة للقضاء، سيفرض الواقع الجديد تحديات في تقييم الأدلة الرقمية؛ فما كان سابقا دليلا دامغا (كفيديو مراقبة يظهر متهما) قد يطعن فيه الآن بدعوى احتمال التزييف، مما يزيد العبء على أجهزة العدالة لإثبات صحة الأدلة أو زيفها. وهذا بدوره قد يطيل أمد المحاكمات أو يؤدي أحيانا لانفلات مجرمين من العقاب إذا ساور الشك القاضي في موثوقية الدليل المرئي/السمعي. ومن هنا يتضح أن تأثير التزييف العميق على الثقة العامة لا يقتصر على الأفراد فحسب، بل يطال مؤسسات الدولة ونظام العدالة بخلق مناخ من الشك المستمر يتطلب موارد وجهود إضافية لحسمه[١٧].

لكل ما سبق، يتبين أن المحتويات الاصطناعية غير التوافقية تمثل تهديدا متعدد الأبعاد للأمن الرقمي والثقة في الفضاء العام. فهي تقوض أسس التواصل الموثوق والمعرفة الصحيحة، وتتيح للجريمة الإلكترونية مستويات غير مسبوقة من الدهاء والفعالية. وقد دفعت هذه المخاطر العديد من الدول إلى الاعتراف بأن سلامة الفضاء السيبراني باتت جزءا لا يتجزأ من الأمن القومي والاجتماعي. وعلى الصعيد القانوني، أوجبت هذه المعطيات التحرك لإيجاد أدوات جنائية ورقابية لكبح إساءة استخدام تقنيات الذكاء الاصطناعي في التضليل والاحتيال، كما سنرى عند عرض الاستجابات التشريعية في المبحث الثاني.

الفرع الثاني: أثر المحتويات الاصطناعية على الحق في الخصوصية وسمعة الأفراد

إذا كان الفرع السابق قد تناول المخاطر "العامة" للتزييف العميق على المجتمع والدولة، فإن هذا الفرع يركّز على المخاطر "الفردية" التي يتعرض لها ضحايا المحتويات الاصطناعية غير التوافقية. فثمة اعتداء مباشر على حقوق الشخص المستهدف في صورته وصوته وخصوصية حياته، بل وكرامته الإنسانية، إلى جانب ما يلحق به من أذى معنوي ومادي. ويمكن إبراز أهم هذه الآثار فيما يأتي:

https://doi.org/10.61353/ma.0210133

أولًا: انتهاك صارخ للخصوصية (Privacy Invasion): يعد نشر صورة شخص أو مقطع له في سياق خاص أو حميمي بدون إذنه انتهاكًا واضحا لخصوصيته حتى لو كانت الصورة حقيقية فكيف إذا كانت الصورة زائفة تماما وذات طابع مشين؟ إن الصور الحميمية غير التوافقية – أي المزيفة دون رضا أصحابها – تمثل شكلاً حديثا من أشكال الاعتداء على الحياة الخاصة للأفراد[١٨]. ففي حالات كثيرة، يقوم الجاني بأخذ صورة وجه الضحية (قد تكون صورة عادية منشورة على حسابها الاجتماعي) ثم يولّفها رقميا على جسد عار في وضع مخل بالآداب، ناشرا إياها على الإنترنت أو مشاركًا إياها عبر مجموعات خاصة. النتيجة أن الضحية تجد نفسها – دون أي ذنب اقترفته – منتهكة الخصوصية بصورة عميقة للغاية، حيث يظهر جسدها (وإن كان جسدا منتحلا) عاريا للعموم. إن مجرد استخدام صورة شخص أو صوته دون موافقته يعدّ بحد ذاته جريمة انتهاك خصوصية يعاقب عليها القانون، لما فيه من استغلال غير مشروع لبياناته الشخصية وصوره. وينطبق هذا حتى لو كانت المادة المنتشرة غير فاضحة؛ إذ يكفي استخدام صورة الشخص بدون إذنه في سياق قد يسيء له ليشكل مساسا بحياته الخاصة[١٩]. ومن الأمثلة الواقعية، قضية نظرتها مجالس الإشراف لدى شركة فيسبوك (ميتا) عام ٢٠٢٤ تتعلق بصور عارية مزيفة لفنانات مشهورات، إذ شددت على حق الأفراد (بمن فيهم الشخصيات العامة) في حماية صورتهم من التشويه الرقمي غير التوافقي. وبذلك، يبرز المحتوى الاصطناعي غير التوافقي كوجه جديد لانتهاك الخصوصية يستلزم حماية خاصة[٢٠].

ثانيا: تشويه السمعة والإساءة المعنوية (Reputation Harm & Emotional Distress): غالبا ما يكون الغرض الأساسي من إنشاء محتوى اصطناعي غير توافقي عن شخص ما هو الإساءة إلى سمعته أو التشهير به. فمثلاً، قد ينشر فيديو مزيف لشخصية اجتماعية أو سياسية وهو يقوم بفعل مشين أو يدلي بتصريحات مهينة بهدف الإضرار باعتباره في نظر الجمهور. ومع الانتشار الفيروسي السريع لمحتويات الإنترنت، قد يجد الضحية نفسه محاطًا باتهامات ووصمة اجتماعية قبل أن تتاح له الفرصة لنفي صحة المقطع أو الصورة. إن الضرر المعنوي الواقع هنا شديد الوطأة؛ إذ تتعرض سمعة الفرد وكرامته للتجريح بناء على مشهد لم يكن يوما جزء منه. وقد بينت إحدى الدراسات أن النساء بشكل خاص يكن ضحايا لتزييف عميق يحمل طابعا جنسيا انتقاميا، بهدف إذلالهن أو الانتقام منهن (كما حصل مع صحفيات وناشطات تعرضن لحملات افتراء بتداول مقاطع إباحية مزيفة تنسب إليهن زورا)[٢١]. حتى وإن استطاع الشخص دحض صحة المحتوى المزيف لاحقًا، فإن الأثر السلبي على سمعته قد يكون قد ترسخ في أذهان الكثيرين، فضلاً عما يعانيه نفسيا من شعور بالعجز والإهانة. وقد أشارت الأستاذة دانييل كيتس سيترون (Danielle Keats Citron): إلى أن "تقنية التزييف العميق أصبحت كسلاح ضد النساء" تحديدًا، في إشارة إلى استغلالها لتشويه سمعتهن والنيل من مكانتهن الاجتماعية. وينسحب الأمر كذلك

على الشخصيات العامة؛ فمثل هذه المقاطع قد تفقد الثقة بشخص برئ عبر وصمه زورا، وهو ما يعدّ شكلاً من أشكال التشهير الجنائي (criminal defamation) الذي يستوجب العقاب. إذاً، يمثل المحتوى المزيف اعتداء على حق الشخص في السمعة الحسنة المكفول قانوناً، ويتقاطع مع جرائم السب والقذف التقليدية وإن اتخذ صورة تقنية مستحدثة[٢٢].

ثالثا: الأضرار النفسية والجسدية المحتملة (Psychological and Physical Harm): لا تقتصر تبعات المحتويات الاصطناعية المسيئة على الأضرار المعنوية فحسب، بل قد تمتد أيضا لتلحق أذى نفسيا بالغا بالضحية قد ينعكس على صحته الجسدية. فالتعرض لمثل هذا التشهير الجنسي أو الاجتماعي الإلكتروني يمكن أن يسبب للضحية صدمة نفسية (trauma) واضطرابات قلق واكتئاب، وشعور بفقدان الأمان والثقة بالآخرين. وقد سجلت بالفعل حالات لضحايا (خصوصا من الفتيات) أصبن بانهيارات عصبية أو اضطررن للانعزال الاجتماعي إثر انتشار صور مزيفة فاضحة لهن[٢٣]. وفي بعض المآسي القصوى، يمكن أن تدفع هذه الضغوط النفسية ضحية حساسة إلى إيذاء نفسها أو محاولة الانتحار هربا من وصمة العار الإلكترونية. كما أن الخوف من أن يكون المرء ضحية تالية لمثل هذه الأفعال قد يولّد حالة عامة من الرعب الإلكتروني تمنع الأفراد (خاصة النساء) من المشاركة الطبيعية عبر الإنترنت أو التعبير عن آرائهم، خشية الانتقام منهم بصناعة محتوى فاضح عنهم. يضاف إلى ذلك احتمال الابتزاز والتهديد؛ إذ قد يستخدم الجاني المحتوى المزيف لابتزاز الضحية ماديا أو جنسيا تحت تهديد نشره على الملأ، وهو ما يضاعف الضرر ويضيف بعداً إجراميا آخر (جريمة الابتزاز)[٢٤]. لذا، تتخطى تأثيرات المحتوى الاصطناعي غير التوافقي مجرد الإحراج لتشكل اعتداء نفسي واجتماعي كبير يستلزم حمايته جنائيا.

رابعا: تداخل مع حقوق المؤلف والملكية الفكرية: قد لا يكون هذا الأثر مباشرا على الشخص المعتدى عليه، لكنه يذكر لإكمال الصورة. فإنتاج محتوى يستخدم صوت، أو صورة شخص ربما يصطدم أيضاً بقوانين حماية حق الاسم والصورة، أو حتى حقوق الملكية الفكرية إذا كانت صورة الشخص علامة تجارية مثلا. في القانون الفرنسي يعد حق الصورة من حقوق الشخصية المحمية، ونشر صورة شخص (حقيقي أو مزيفة) على نحو يسيء له بدون إذنه يعدّ تعديا يعطيه الحق في التعويض. كما أن تركيب صوت فنان مثلاً لأداء أغنية بدون موافقته قد يثير مسائل تتعلق بحقوق الأداء العلني وحقوق المؤلف. صحيح أن هذه الجوانب أقرب للمسؤولية المدنية، لكنها تظل من ضمن الآثار المترتبة على الظاهرة التي قد تدعم توجه التجريم لتوفير حماية أشمل[٢٥].

استنادا إلى ما تقدم، يتضح أن المحتويات الاصطناعية غير التوافقية تفضي إلى طيف واسع من الأضرار الفردية التي تمس حقوقاً أساسية للأشخاص. فهي تمثل اعتداء مزدوجا: فمن جهة هي اعتداء على حق الخصوصية عبر السطو على الهوية البصرية/السمعية للفرد واستغلالها بدون رضاه؛ ومن جهة أخرى هي اعتداء

على حقه في الكرامة والسمعة عبر تزييف الواقع بما يسبب له الإهانة والأذى المعنوي. ولا شك أن جسامة هذه الانتهاكات تسوغ تدخل القانون الجنائي لردعها وحماية المجتمع والأفراد منها. وقد أقرت العديد من المصادر القانونية الدولية بشرعية تقييد حرية التعبير والتقنية في هذا المجال حمايةً لحقوق الضحايا؛ إذ يعد فرض قيود على هذا المحتوى أمرا مشروعا لحماية الأفراد من نشر صورهم الجنسية بدون موافقتهم. وعليه، انتقل الجدل من مجرد توصيف الضرر إلى البحث في أنجع السبل القانونية للتصدي له، وهو ما سيكون موضوع المبحث الآتي الذي سيتناول بالتفصيل كيف تعاملت قوانين فرنسا والإمارات والعراق مع هذه الظاهرة عبر التجريم والعقاب وإجراءات الملاحقة.

المبحث الثاني: الإطار القانوني للحماية الجنائية من المحتويات الاصطناعية غير التوافقية

في ضوء ما تقدم من مخاطر جسيمة تسببها المحتويات الاصطناعية غير التوافقية، تبدو الحاجة ملحة لبحث الأدوات القانونية الجنائية المتاحة لمواجهتها. يركز هذا المبحث على استعراض وتحليل النهج القانوني الجنائي الذي اتخذته كل من فرنسا والإمارات والعراق في التصدي لهذه الظاهرة. ويتضمن ذلك جانبين رئيسين: الشق الموضوعي للحماية الجنائية (أي تجريم الأفعال المرتبطة بإنتاج أو نشر المحتوى الاصطناعي غير التوافقي وبيان أركان الجرائم والعقوبات المقررة لها)، والشق الإجرائي للحماية (أي آليات كشف هذه الجرائم وجمع الأدلة بشأنها وإجراءات الملاحقة القضائية، بما في ذلك التعاون الدولي). وسيتم تناول كل شق في مطلب منفصل ضمن هذا المبحث.

المطلب الأول: الإطار الموضوعي للحماية (نحو تجريم المحتويات الاصطناعية غير التوافقية)

يتعلق هذا المطلب بكيفية تناول القوانين الجنائية محل الدراسة للفعل المتمثل في إنشاء أو توزيع المحتوى الاصطناعي الزائف بدون توافق. سنستعرض أولاً الأركان والعناصر المكونة للجريمة في كل نظام (الفرع الأول)، ثم ننتقل لعرض الآثار القانونية المترتبة على ارتكاب الفعل من حيث العقوبات الجنائية المقررة والتدابير الاحترازية المكملة (الفرع الثاني). وستتخلل ذلك مقارنة بين المواقف التشريعية في فرنسا والإمارات والعراق، مع الإشارة إلى أوجه القصور أو القوة في كل منها.

الفرع الأول: أركان الجريمة (الركن المادي والركن المعنوي)

إن تجريم فعل ما في القانون الجنائي يقتضي تحديد الأركان الأساسية التي لا يقوم إلا بها: وتشمل عادةً الركن المادي والركن المعنوي. وفي سياق المحتويات الاصطناعية غير التوافقية، ظهرت عدة مقاربات في التشريعات المقارنة لتحديد هذه الأركان بوضوح، لاسيما مع كون الفعل جديدًا نسبيا. وفيما يلي تحليل لكيفية تعريف المشرع لهذه الجريمة وعناصرها في فرنسا والإمارات، ووضع القانون العراقي الحالي تجاهها:

https://doi.org/10.61353/ma.0210133

أولًا: الركن المادي للجريمة: يتمثل الركن المادي عموما في سلوك إنتاج أو نشر محتوى مزيف رقميا لشخص بدون رضاه. وقد يأخذ هذا السلوك صورا متعددة: ابتداء من صنع المحتوى الاصطناعي ومرورا بحيازته أو التخطيط لاستعماله، وانتهاء بنشره أو توزيعه على الآخرين .والملاحظ من التجارب المقارنة أن التركيز انصب على تجريم فعل النشر أو التوزيع تحديدا كونه الحلقة التي تتحقق بها العلانية والضرر، مع عدم إغفال معاقبة من يقوم بالتصنيع ذاته إن كان لديه قصد الإضرار.

في القانون الفرنسي, قبل عام ٢٠٢٤، كانت المادة ٢٢٦-٨ من قانون العقوبات الفرنسي تُجرم نشر "مونتاج" لشخص دون إذنه إذا لم يذكر أنه مركّب. لكن عبارة "مونتاج" أثارت جدلًا حول انطباقها على التلاعب بواسطة الذكاء الاصطناعي، نظرا لأن التفسير الضيق ربما يحصرها في المزج التقليدي للصور بالفوتوشوب دون أن يشمل التوليد الاصطناعي[٢٦]. لذلك جاء تعديل ٢٠٢٤ ليضيف صراحة تجريم نشر أي محتوى مرئي أو سمعي منشأ بالمعالجة الخوارزمية يمثل صورة أو صوت شخص دون موافقته إلا إذا كان واضحا أو مصرحا بأنه مصطنع. إذًا، حدد المشرع الفرنسي النشاط المادي المحظور بأنه نشر أو مشاركة المحتوى المزيف. أما مجرد إنشاء المحتوى دون مشاركته علنا، فلا يبدو أنه مجرم بذاته في النص (إلا لو اندرج كتحضير أو شروع لجريمة النشر). ذلك منطقي لأن الضرر يتحقق بالنشر الذي يطلع عليه الغير[٢٧]. إضافة لذلك، استحدث المشرع مادة ٢٢٦-٨-١ لعام ٢٠٢٤ خاصة بالمحتوى الجنسي المزيف حرمت نشر أي محتوى إباحي مصطنع لشخص دون موافقته مطلقا (حتى لو كان واضح الزيف أو مصرحا به). ما يسترعي الانتباه هنا أن المشرع ألغى الاستثناء المتعلق بوضوح المحتوى في الحالة الجنسية تشديدا للحماية، باعتبار أن مجرد تداول صورة جنسية لشخص من دون رضاه يشكل اعتداء كافيا حتى لو علم أنها مزيفة. وخلاصة القول، يتمحور الركن المادي في فرنسا حول فعل النشر العلني للمحتوى الاصطناعي غير التوافقي. أما النتيجة الاجرامية المفترضة فهي المساس بحق الشخص (خصوصيته/شرفه) أو خداع الجمهور، لكن القانون الفرنسي لا يشترط وقوع ضرر مادي معين؛ إذ تقوم الجريمة بمجرد تحقق فعل النشر دون موافقة. ويلاحظ أيضا اشتراط انتفاء الإقرار بكون المحتوى مزيف (إلا في المحتوى الجنسي حيث لا عبرة لذلك). فهذا الإقرار إن وجد ينفي عن الفعل صفة الخداع ومن ثم لا يعاقب عليه (مثال ذلك: فيديو ساخر يصرح في مقدمته أنه محاكاة ساخرة).

أما في القانون الإماراتي, لا يوجد نص منفرد يعرف جريمة "التزييف العميق" تحديدا، لكن المنظومة الإماراتية تشتمل على عدد من الجرائم التي يغطي مجموعها الأفعال المكونة لهذا السلوك. فعلى صعيد النشر غير المشروع للمحتوى، لدينا عدة أفعال مجرمة: نشر ما من شأنه المساس بخصوصية الآخرين، أو حياتهم الخاصة عبر وسائل تقنية (ويدخل فيه نشر صور، أو أخبار عن شخص بغير رضاه)، وكذلك نشر أخبار، أو شائعات كاذبة عبر الشبكة بقصد الإضرار أو خداع الجمهور. وبالتالي، نشر فيديو مزيف يشهر بشخص قد يقع تحت تجريم التشهير الإلكتروني ونشر ما يسيء إلى الغير. أما فعل الإنشاء للمحتوى المزيف، فإن القانون

الإماراتي تناوله بطريقة غير مباشرة عبر تجريم صنع أو تعديل برنامج إلكتروني بقصد نشر معلومات أو أخبار كاذبة. إذ تجرم المادة ٥٤ من قانون مكافحة الجرائم الإلكترونية إنشاء برامج (روبوت إلكتروني) أو تعديلها لتمكين نشر البيانات الزائفة[٢٨] . وهذا النص ابتكر بالأساس لمكافحة الحسابات الآلية المضللة (البوتات)، لكنه يمكن أن ينطبق في حالة تطوير أدوات Deepfake أو استخدام برمجيات لهذا الغرض بقصد نشر مخرجات كاذبة. إذاً، في الإمارات يمكن ملاحقة من يصنع المحتوى المزيف باعتباره شارك في عملية الخداع ونشر الأخبار الكاذبة بشكل تقني (وتصل العقوبة لسجن سنتين وغرامة حتى مليون درهم لهذه الأدوات). فضلاً عن ذلك، فإن إنتاج أو حيازة مواد إباحية أو غير أخلاقية لتوزيعها يعاقب عليه أيضا في إطار قوانين الآداب العامة. عموماً، يغطي القانون الإماراتي الركن المادي عبر حزمة من الجرائم: نشر ما ينتهك الخصوصية (كصور شخص دون إذنه)، نشر ما يشهر بالغير (القدح والذم)، نشر الأخبار الكاذبة والإشاعات، تزوير المستندات أو الصور الإلكترونية، والمواد الإباحية. وبذلك، رغم غياب مسمى صريح لجريمة "المحتوى الاصطناعي غير التوافقي"، فإن الأفعال المكونة له مجرمة عبر أوصاف متعددة. ومن الناحية التقنية، لا يشترط تحقق ضرر خاص لقيام هذه الجرائم، فيكفي قيام فعل النشر أو الإنشاء الممنوع بالقصد الجرمي. كما أن مجرد تداول المحتوى ضمن مجموعة إلكترونية مغلقة قد يعدّ علانية إذا تجاوز النطاق الخاص، وفق تفسير المحاكم لمفهوم العلانية في مواقع التواصل.

وبخصوص القانون العراقي, وحتى تاريخ إعداد هذا البحث، لا يوجد نص صريح في قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ (أو أي قانون نافذ آخر) يُجرم إنشاء أو نشر المحتويات الاصطناعية غير التوافقية بشكل خاص. لذا فإن أي ملاحقة لمثل هذه الأفعال ستتم عبر تكييفها ضمن أطر الجرائم التقليدية القائمة. بالنسبة لفعل النشر: يمكن أن ينطبق عليه جريمة القذف والتشهير العلني المنصوص عليها في المادتين ٤٣٣-٤٣٤ عقوبات. فالمادة ٤٣٣ تعرف القذف بأنه "إسناد واقعة معينة إلى الغير بإحدى طرق العلانية من شأنها لو صحت أن توجب عقاب من أسندت إليه أو احتقاره عند اهل وطنه"[٢٩]. ونشر فيديو مزيف لشخص يظهره مرتكبا فعلاً جرميا أو مشينا يندرج حرفيا تحت هذا التعريف (إسناد واقعة تستوجب عقاب أو احتقار لو كانت صحيحة). كذلك قد يندرج نشر صورة فاضحة مزيفة لشخص ضمن القذف العلني لأنه ينطوي على إسناد أمر معيب له علنا. وبذلك يمكن استخدام مواد التشهير التقليدية لمعاقبة النشر المزيف المسيء. أما فعل إنشاء المحتوى المزيف، فمن الناحية الواقعية يمكن ملاحقته كنوع من أنواع التزوير أو صنع دليل مزيف إذا استخدم في إجراءات رسمية. لكن إن لم يصل الأمر إلى مرحلة استخدامه ونشره، سيصعب تجريم مجرد الإنشاء في ظل مبدأ لا جريمة بلا نص. اذ أن استخدام القواعد العامة في القانون الجنائي لمواجهة جرائم الذكاء الاصطناعي يصطدم بمبدأ الشرعية[٣٠]. بمعنى أن سكوت المشرع العراقي عن وصف هذا الفعل صراحة قد يخلق ثغرة لو حاول القاضي معاقبة فعل لم يجرمه القانون بنص واضح. ومع ذلك، قد يحاول القضاء التوسع في تفسير النشر العلني ليشمل أي مشاركة عبر الإنترنت، ولعل فعل النشر بصيغته الإلكترونية الحديثة

https://doi.org/10.61353/ma.0210133

سيغطى قريبا عبر قانون جرائم معلوماتية جديد، حيث أعيد تقديم مشروع قانون الجرائم الإلكترونية إلى البرلمان العراقي في أواخر ٢٠٢٢. ويتضمن هذا المشروع تجريم الأفعال التي من شأنها "المساس بالنظام العام أو السمعة" عبر الإنترنت بأحكام عامة وواسعة قد تشمل المحتوى المزيف. لكن هذا المشروع واجه انتقادات شديدة لخشيه المساس بحرية التعبير ولم يقر بعد.

ثانيا: الركن المعنوي للجريمة: أما من حيث القصد الجنائي (الركن المعنوي)، فإن الجرائم محل النقاش يغلب عليها الطابع العمدي. أي أن ارتكاب فعل إنشاء أو نشر محتوى مزيف يتطلب توافر علم وإرادة لدى الجاني بأن هذا المحتوى غير حقيقي وأن الشخص المعني لم يوافق عليه. وغالبا ما يكون الدافع هو الإضرار بالغير أو تحقيق منفعة غير مشروعة.

فرنسا, تشترط توافر القصد الجنائي العام؛ أي علم الناشر بأن المحتوى مزيف وأنه ينشره دون إذن صاحب الشأن. فإذا أثبت المتهم أنه كان يعتقد بخطأ أن المحتوى حقيقي (مثلاً قام بإعادة نشر فيديو دون علم بأنه مزيف)، فقد ينتفي القصد لديه وبالتالي تنتفي الجريمة عمداً، وإن كان قد يساءل عن إهمال محتمل في سياق آخر. كذلك وضع المشرع الفرنسي استثناء لمن يصرح علناً بأن المحتوى مركب، ما يعني عدم توافر نية الخداع أو الإيهام. في المقابل، بالنسبة للمحتوى الجنسي المزيف، ألغى الاستثناء مما يدل ضمنيا على افتراض سوء النية في كل نشر لمحتوى جنسي دون إذن الشخص — فمن ينشر صورة فاضحة لشخص قطعا يقصد الإساءة حتى لو زعم المزاح أو السخرية[٣١]. ومن الجدير ذكره أن القانون الفرنسي في جرائم التشهير التقليدية يتيح دفع "حسن النية" للمتهم كسبب إعفاء إذا تمكن من إثبات عدم تعمده الإساءة؛ ولكن في حالة التزييف العميق، يصعب تصور نشر كهذا عن حسن نية إلا في إطار فني واضح. إذاً، القصد الخاص المطلوب غالبا هو نية الإضرار بكرامة الشخص أو سمعته أو تضليل الجمهور. أما إذا كان النشر بقصد الفكاهة أو الفن بدون نية الإساءة وثبت ذلك بوضوح، فقد يحول دون الإدانة، إما لانطباق الاستثناء (إن كان معلناً) أو لانتفاء القصد الجرمي رغم تحقق الفعل ماديا[٣٢].

أما في الإمارات, معظم الجرائم الإلكترونية المتعلقة بالمحتوى في القانون الإماراتي تشترط العمد والقصد الجنائي. فمثلاً، جريمة القذف الإلكتروني عبر المادة ٤٤ من قانون مكافحة الشائعات تتطلب أن يكون النشر بقصد المساس بكرامة الغير. وكذلك جريمة نشر معلومات بقصد الإضرار بالسمعة أو بالمصالح الوطنية تشترط قصداً خاصا يتمثل في علم الجاني بكذب المحتوى ورغبته في تداوله للإضرار. من ثم لو قام شخص بإعادة نشر فيديو مزيف بدون أن يعلم بزيفه ومن غير قصد للإساءة، فالأرجح أنه يعفى لانتفاء القصد الجرمي (مع بقاء إمكانية مساءلته مدنيا عن الضرر). أما قصد التربح أو الابتزاز فيعد ظرفاً مشددا أو جريمة مستقلة (كالابتزاز المقرون بالتهديد بنشر محتوى، أو الاحتيال للحصول على مال عبر المحتوى المزيف). وتجدر الإشارة أن القانون الإماراتي يتسم بالحزم تجاه الجرائم العمدية عبر الإنترنت، وهو يفترض

https://doi.org/10.61353/ma.0210133

العلم غالبا إذا كانت الظروف تشير إلى ذلك. فمجرد نشر شخص لصورة غيره الخاصة دون إذنه يدل على علمه بعدم الإذن وقصده انتهاك الخصوصية، ما لم يثبت العكس بشكل استثنائي (كأن يثبت أنه اعتقد رضاه). عموما، الخطأ غير العمدي (كالإهمال في التحقق من صحة فيديو قبل نشره) غير معاقب عليه جنائيا في هذه الحالة؛ لأن الجرائم ذات الصلة تتطلب قصداً مباشرا أو احتماليا. ويمكن القول إن الركن المعنوي في الإمارات أشد وضوحا منه في فرنسا، كون النصوص جاءت مرتكزة على الفعل العمدي؛ فمثلاً المادة ٤٥ من قانون الجرائم الإلكترونية تجرم استخدام التقنية "بقصد" المساس بخصوصية شخص أو حياته الخاصة. وكذلك المادة ٥٤ تجرم إنشاء برامج بقصد نشر الأخبار الكاذبة. فالقصد الخاص (نية المساس أو الخداع) عنصر جوهري للإدانة.

وفيما يتعلق بالقانون العراقي، فأن جريمة القذف (التشهير) التقليدية تتطلب تحقق القصد الجنائي العام بأن يسند الجاني الواقعة وهو يعلم أنها ستسبب احتقارا للمجني عليه. فإذا ثبت أن الناشر كان يظن الواقعة صحيحة (أي خدع هو الآخر بالمحتوى)، فقد يدفع بانتفاء القصد الجرمي عنه. لكن عمليا القضاء قد يأخذ بقرينة العلم إذا كان المحتوى غريبا أو مريبا وكان الناشر على صلة عداء بالمجني عليه. عموما، لا تعاقب قوانين العقوبات على الإهمال في النشر فيما يخص السمعة، لذا من ينشر مادة مسيئة بزعم المزاح أو التقليد دون قصد الإساءة قد لا تقبل منه هذه الدفوع بسهولة إلا في ظروف واضحة. أيضا هناك جرائم نشر مطلقة لا تكترث للدافع مثل المادة ٤٠٣ عقوبات (نشر المطبوعات المخلة بالحياء) التي لا تشترط قصد الإساءة لشخص محدد بل يكفي تعمد نشر مادة فاحشة للجمهور. لذا نشر صورة إباحية (حتى لو مزيفة لشخص) قد يقع تحت طائلتها لمجرد تعمد النشر بغض النظر عن استهداف شخص بعينه. ومع ذلك، في تكييف التزييف العميق كشكل من أشكال التزوير أو اختلاق الأدلة قد يثير تساؤل القصد. فهل يعامل كمن زور مستنداً وهو عالم بتزويره؟ نعم، فمن يختلق فيديو مزيف يعلم تماماً أنه غير صحيح. إذا القصد متحقق. وإن قوربت المسألة من زاوية انتحال الهوية (رغم عدم وجود نص في العراق يجرم مجرد الانتحال إلا في حالات خاصة)، فإن انتحال شخصية آخر بإنتاج محتوى يوهم أنه هو، يستلزم حتما قصداً جنائيا (إما خداع الجمهور أو الإساءة للمنتحل).

بالنتيجة، تشترك جميع الأنظمة محل الدراسة في اشتراط الركن المعنوي العمدي في جرائم المحتوى الاصطناعي غير التوافقي. وعادة ما يكون هذا القصد هو القصد الجرمي الخاص المتمثل في نية الإضرار بالغير (سواء بسمعته أو خصوصيته) أو نية خداع العامة وتضليلهم. وهذا طبيعي نظرا لخطورة الفعل؛ فالقانون الجنائي يتدخل عندما يتعمد شخص إساءة استخدام حرية التعبير أو التقنية للتعدي على حقوق الآخرين. أما الحالات غير العمدية أو التي قد يبدو فيها الناشر حسن النية، فيفترض معالجتها خارج الإطار الجنائي (كأن يطالبه المتضرر بإزالة المحتوى أو يرفع عليه دعوى تعويض مدني). وفي بعض التشريعات مثل فرنسا، أُعطي للقضاء

دور في تقدير قصد الخداع من مظهر المحتوى نفسه: هل هو بديهي الزيف أم قد ينخدع به الناس، لتحديد ما إذا كان النشر يستحق العقاب. ولكن تلك مساحة فضفاضة تركت لاجتهاد المحاكم. وبشكل عام، فإن وضوح نصوص التجريم واستيعابها للتقنية الحديثة يقلل الحاجة للاجتهاد التأويلي ويؤمن احترام مبدأ شرعية الجرائم والعقوبات، وهو ما حرص عليه المشرع الفرنسي بإضافة نصوص خاصة عام ٢٠٢٤.

الفرع الثاني: الأثر القانوني المترتب على الفعل (العقوبات والتدابير الاحترازية)

بعد تحديد ما يشكل جريمة في نطاق المحتويات الاصطناعية غير التوافقية، تأتي مسألة العقوبات المقررة على مرتكبي هذه الجريمة والتدابير الإضافية الممكن اتخاذها لحماية المجتمع والضحايا. وسنستعرض في هذا الفرع العقوبات المنصوص عليها في القانون الفرنسي والإماراتي (والتي تتميز بتدرجها بحسب جسامة الفعل ووسيلة النشر)، ثم نعرج على موقف القانون العراقي الحالي من حيث العقوبات الممكن تطبيقها على الجرائم التقليدية الموافقة، وصولاً إلى مناقشة التدابير الاحترازية (مثل إزالة المحتوى وحجب المواقع والتعويض وغيرها) في الأنظمة الثلاثة.

أولا: العقوبات الجنائية المقررة:

في القانون الفرنسي, عدت التعديلات الجديدة لعام (٢٠٢٤) على قانون العقوبات الفرنسي جرائم المحتوى الاصطناعي غير التوافقي من فئة الجنح (délits) وحددت لها عقوبات سالبة للحرية وغرامات مالية متفاوتة. فبموجب المادة ٢٢٦-٨ المعدلة: يعاقب على نشر المحتوى المزيف لشخص دون موافقته بالسجن لمدة تصل إلى سنة واحدة و/أو غرامة تصل إلى ١٥,٠٠٠ يورو. وترتفع العقوبة إلى الحبس حتى سنتين وغرامة حتى ٤٥,٠٠٠ يورو إذا ارتكب الفعل عبر خدمة عامة إلكترونية (كوسائل التواصل الاجتماعي أو موقع إنترنت عام). هذا التشديد للأفعال عبر الإنترنت سببه أن العلانية والمدى يكونان أكبر، فاعتبر ظرفا مشددا. أما بالنسبة للمحتوى الجنسي المزيف (المادة ٢٢٦-٨-١ الجديدة): فالعقوبة الأساسية الحبس حتى سنتين وغرامة حتى ٦٠,٠٠٠ يورو، وتصبح حتى ٣ سنوات وغرامة ٧٥,٠٠٠ يورو إذا تم النشر عبر وسيلة إلكترونية عامة. نلاحظ أن العقوبة هنا أشد من نظيرتها في المحتوى العادي، وتعادل تقريبا ضعف العقوبة الأساسية، مما يعكس خطورة الانتهاك الجنسي لخصوصية الأفراد. هذه العقوبات تعد رادعة ومتناسبة مع جسامة الأفعال، مع الإبقاء عليها ضمن نطاق الجنح وليس الجنايات (أي أن المشرع لم يعتبرها جريمة أخطر من الاعتداء الجسدي مثلا). وإلى جانب السجن والغرامة، نص القانون الفرنسي عموما على عقوبات تبعية محتملة مثل مصادرة المعدات المستخدمة في الجريمة، وحجب الحسابات الإلكترونية التي نشرت المحتوى، ونشر الحكم في الصحف، لكنها خاضعة لتقدير القاضي وليست تلقائية.

أما في القانون الإماراتي, يعد التشريع الإماراتي متشددا نسبيا في العقوبات المالية على الجرائم الإلكترونية مقارنة بغيره. هناك عدة مواد يمكن تطبيق عقوباتها كما أسلفنا: اذ انه يعاقب على جريمة التشهير/السب الإلكتروني في المادة ٤٤ من قانون مكافحة الشائعات والجرائم الإلكترونية الاتحادي (٣٤ لسنة

٢٠٢١) , إذ عاقبت على السب أو القذف عبر نظام معلوماتي الكتروني بالحبس مدة تصل إلى سنة وغرامة بين ٢٥٠,٠٠٠ و٥٠٠,٠٠٠ درهم. وهذا يشمل حالة نشر محتوى مزيف يسيء لشخص (كفيديو أو صورة تشهيرية)، إذ سيعد شكلاً من القذف المعلوماتي. وفيما يتعلق بانتهاك الخصوصية الإلكتروني, يعاقب بحسب المادة ٤٥ بالحبس مدة لا تقل عن ٦ أشهر والغرامة التي لا تقل عن (٢٠٠,٠٠٠) مائتي ألف درهم ولا تزيد على (١,٠٠٠,٠٠٠) مليون درهم كل من استخدم الوسائل التقنية للتعدي على خصوصيات الغير بنشر أخبارهم أو صورهم بدون إذن إذا سببت ضررا. وبالتالي، نشر صورة شخص (حتى لو حقيقية) دون رضاه للتشهير به يعاقب في هذا الإطار. أما لو كانت الصورة مزيفة، فيمكن وصفها أيضا انتهاك خصوصية فضلاً عن أنها كاذبة، فتتداخل النصوص ويمكن تطبيق الأشد. وإذا استخدم المحتوى المزيف للحصول على منفعة أو مال بالخداع، فتطبق المادة ٤٠ الخاصة بـ"الاحتيال الإلكتروني" التي تقرر الحبس (حد أدنى سنة) وغرامة ٢٥٠,٠٠٠ إلى ١,٠٠٠,٠٠٠ درهم لمن احتال باستعمال وسيلة إلكترونية. وهذه عقوبة مشددة مقارنة بالاحتيال العادي (الذي عقوبته في قانون العقوبات الإماراتي الحبس أو السجن حتى سنتين وفق مقدار الضرر)، مما يظهر التشدد مع استخدام التقنية في الجريمة. وفيما يخص المواد الإباحية, يحظر القانون الإماراتي تماما إنتاج أو نشر مواد إباحية أو تتعلق بالدعارة في المادة (٣٤) اذ يعاقب بالحبس والغرامة التي لا تقل عن (٢٥٠,٠٠٠) مائتين وخمسين ألف درهم ولا تزيد على (٥٠٠,٠٠٠) خمسمائة ألف درهم)، كل من أنشأ أو أدار موقعاً إلكترونياً أو أشرف عليه أو بث أو أرسل أو نشر أو أعاد نشر أو عرض عن طريق الشبكة المعلوماتية مواد إباحية وكل ما من شأنه المساس بالآداب العامة.

نلاحظ أن الإمارات تميل إلى العقوبات المالية الضخمة (مئات الآلاف من الدراهم) فضلاً عن العقوبات السالبة للحرية المتوسطة (أشهر أو سنوات قليلة). وهذا يعزى إلى سياستها التشريعية في الردع عبر ضرب الجناة ماليا بقوة. كما يتميز القانون الإماراتي بنظام ظروف مشددة متعددة مثل: إذا كان المجني عليه طفلاً أو أنثى (في بعض الجرائم تضاعف العقوبة)، أو إذا ارتكب الجريمة جماعة إجرامية منظمة. كذلك تطبق أحكام العود المشددة عند التكرار. في المجمل، قد يواجه من يقوم بالتزييف العميق المسيء في الإمارات عقوبات جمع متعددة إذا انطبقت أفعال مختلفة (مثال: شخص زور فيديو ثم نشره بعد ذلك ابتز به الضحية فهو قد جمع بين جرائم التزوير الإلكتروني، ونشر ما يمس السمعة، والابتزاز)، مما قد يرفع مجموع العقوبات إلى سجن لعدة سنوات وغرامات بملايين الدراهم. وهذا الإطار الصارم يعكس نهج الإمارات في حماية الفضاء الإلكتروني بقوة القانون.

وبخصوص القانون العراقي, وكما بينا، لا توجد عقوبات خاصة مستحدثة لهذه الجريمة، لذا يعتمد الأمر على مواد قانون العقوبات, اذ تعاقب المادة ٤٣٣ من قانون العقوبات العراقي على القذف بالحبس مدة قد تصل إلى سنة واحدة وبالغرامة أو بإحدى هاتين العقوبتين. والمادة ٤٣٤ تعاقب السب (الإهانة)

بالحبس حتى ٣ أشهر أو الغرامة. وهناك مادة ٤٣٥ تشدد العقوبة إلى حد ٦ أشهر إذا تم القذف أو السب بواسطة الهاتف أو الرسالة (وأعتقد أنه ينطبق الآن على الرسائل الإلكترونية أيضا)، ولكنها تبقى أقل من سنة. وبالتالي، أقصى عقوبة للتشهير الإلكتروني حاليا يمكن أن يواجهها من ينشر محتوى مزيف مسيء هي الحبس لمدة سنة (وهذا في حال القذف بإسناد أمر جنائي للمجني عليه). وإذا رافق نشر المحتوى تهديد للضحية (كأن يقول إن لم تدفع سأنشر الفيديو)، فهذه جريمة تهديد أو ابتزاز منفصلة عقوبتها وفق المادة ٤٣٠ عقوبات تصل إلى السجن مدة لا تزيد على ٧ سنوات. اما بخصوص النشر المخل بالحياء فالمادة ٤٠٣ عقوبات تعاقب بالحبس حتى سنتين كل من نشر صورا أو كتابات أو أفلاما مخلة بالحياء أو دعائية للجنس. لو رأى القاضي فيديو إباحي مزيف لشخص أنه يندرج تحت هذا (بغض النظر عن رضا أو عدم رضا صاحب الصورة لأنه صورة مزيفة أصلاً)، يمكن إعمال هذه المادة أيضا، وتصل العقوبة لسنتين.

بصورة عامة، يتبين أن العقوبات المتاحة في العراق حاليا أقل شدة مما هي عليه في فرنسا والإمارات في جرائم النشر المسيء. فالحبس سنة للتشهير أقل بكثير من ٢–٣ سنوات في القوانين المقارنة، وغرامات العراق (إن حكم بها) رمزية بضع مئات آلاف الدنانير، مقارنة بعشرات الآلاف من اليورو أو نصف مليون درهم في الإمارات. هذا الفارق قد يجعل العقوبة غير متناسبة مع الضرر في حالات التزييف العميق الخطيرة. ولا ننسى أن كثيرا من الجرائم المعلوماتية يمكن أن يفلت مرتكبها بأحكام مع وقف التنفيذ إن لم يكن عائداً أو إن كانت عقوبتها الحبس البسيط، ما لا يحقق الردع الكافي. من جهة أخرى، الدعوى المدنية بالتعويض متاحة للمجني عليه في العراق للمطالبة بجبر الضرر المعنوي، لكن مبالغ التعويض التي تحكم بها المحاكم عادة محدودة أيضا ولا ترقى للأضرار الفعلية. وهذا كله يستدعي إعادة نظر تشريعية لتشديد العقوبات بما يلائم خطورة التزييف العميق وانتشاره السريع.

ثانيا: التدابير الاحترازية وحماية الضحايا:

إلى جانب العقوبات الجنائية التقليدية، من المهم بحث التدابير الأخرى التي يمكن للجهات القضائية أو التشريعية اتخاذها لمنع استمرار الضرر وحماية الضحية والمجتمع من تبعات المحتوى الاصطناعي غير التوافقي. من هذه التدابير:

١. إزالة المحتوى وحظره: في فرنسا، تعد إزالة المحتوى غير القانوني، بما في ذلك الصور والفيديوهات المزيفة (deepfakes)، مسؤولية مشتركة بين السلطات القضائية والإدارية. ورغم أن قانون العقوبات الفرنسي لا يتضمن نصا صريحا يلزم بحذف المحتوى، إلا أن المحاكم يمكن أن تأمر بإزالته في سياق الأحكام القضائية أو بطلب مستعجل. كما يمنح القانون الفرنسي صلاحيات للمجلس الأعلى للإعلام السمعي البصري (CSA) للتنسيق مع المنصات الرقمية من أجل إزالة

المحتوى الضار أو غير القانوني. وقد صدر قانون حديث يجرم استخدام "التزييف العميق" لأغراض إباحية أو دون موافقة الضحية، ويتيح للمنصات مثل Meta التدخل لحذف المحتوى المتعلق وتضمينه ببصمات رقمية لمنع إعادة تحميله[٣٣]. في الإمارات، المادة ٥٩ من قانون الجرائم الإلكترونية تمنح المحكمة سلطة حجب الموقع أو المنصة التي تستضيف المحتوى المخالف. كما تتعاون هيئة تنظيم الاتصالات والحكومة الرقمية في الإمارات (TDRA) بشكل سريع وفعال مع منصات التواصل الاجتماعي لإزالة المحتوى الضار، لا سيما بناء على توجيهات أمنية أو حكومية. وقد فعلت الهيئة عدة اتفاقيات تعاون مع منصات مثل TikTok للتعامل مع المحتوى الذي يشكل خطرا على السلامة الرقمية أو يتنافى مع القيم الوطنية[٣٤]. اما في العراق، لا آلية واضحة وسريعة لإزالة المحتوى من الإنترنت، سوى مخاطبة إدارة المواقع (وهو أمر غير فعال غالبا) أو حجب الموقع بالكامل عن طريق وزارة الاتصالات. لكن الحجب الشامل حل ثقيل وقد يستخدم في حالات قصوى ويصيب غالبا خدمات مشروعة بأضرار جانبية. لذا لا بد من وضع آلية قانونية سريعة مثل أوامر قضائية مستعجلة إلى مزودي الخدمة الدولية لإزالة محتوى مزيف يتعلق بمقيمين في العراق، وربط العراق باتفاقيات تعاون مع الشركات التقنية.

٢. حماية هوية الضحايا ومنع انتشار الضرر: قد تحتاج المحاكم أحيانًا لإصدار أوامر تحفظية بحظر نشر الفيديو أو الصور موضوع الدعوى في الإعلام أثناء سير القضية لمنع زيادة الضرر. أيضا ربما يتطلب الأمر السماح للضحايا بتغيير أسمائهم أو هوياتهم في بعض الحالات القصوى لحمايتهم من الوصمة الإلكترونية (هذه إجراءات مدنية/إدارية وليست جنائية تماما لكنها ذات صلة بحماية الضحية). في فرنسا، ظهر مفهوم "الحق في النسيان" كجزء من قوانين حماية البيانات، وخصوصا بعد صدور قرار محكمة العدل الأوروبية في قضية (Google Spain) 2014، ما أتاح للأفراد المطالبة بإزالة نتائج البحث التي تحتوي على معلومات قديمة أو مضللة تمس حياتهم الخاصة. وقد تم تضمين هذا الحق ضمن اللائحة الأوروبية العامة لحماية البيانات (GDPR) التي تطبقها فرنسا بشكل صارم[٣٥]. أما في الإمارات، فإن قوانين مكافحة الجرائم الإلكترونية تمنح السلطات صلاحيات لمنع المضايقات الإلكترونية، وتتيح للضحايا تقديم شكاوى رسمية لحذف المحتوى أو حجب المواقع. كما يمكن فرض قيود على الجناة من التواصل مع الضحية إلكترونيا، في نمط مشابه لأوامر عدم التعرض القضائية التقليدية.

٣. مصادرة الأجهزة والبرامج المستخدمة: كل من فرنسا والإمارات تجيز مصادرة أدوات الجريمة. فالقاضي الفرنسي يستطيع مصادرة الحاسوب أو الهاتف المستخدم في نشر المحتوى المزيف[٣٦]. وفي الإمارات، المادة ٥٦ من قانون الجرائم الإلكترونية تجيز مصادرة الأجهزة أو إغلاق

الحسابات أو المواقع المتعلقة بالجريمة. هذه التدابير تمنع الجاني من تكرار فعله بسهولة وتظهر جدية الردع.

في ضوء ما سبق، يتضح أن فرنسا وضعت حديثا إطارا عقابيا صريحا ومتكاملاً نسبيا لتجريم المحتويات الاصطناعية غير التوافقية ومعاقبة مرتكبيها بعقوبات حبسية ومالية مناسبة، مع اهتمام خاص بالمحتوى الجنسي. الإمارات من جهتها تعتمد على ترسانة قوية من مواد قانونية متفرقة لكنها فاعلة، تَغلّظ العقاب خاصة المالي وتشمل مختلف جوانب السلوك الإجرامي، مدعومةً بإمكانية إجراءات إضافية كحجب المواقع ومصادرة الأجهزة. أما العراق فيبدو حاليا الحلقة الأضعف في هذه المقارنة، إذ تنحصر استجابته ضمن نصوص قديمة وعقوبات مخففة نسبيا، دون أدوات حديثة للإزالة أو المنع، مما يجعله بحاجة ماسة لتحديث تشريعي لرفع سقف العقوبات ورفدها بتدابير احترازية صالحة للعصر الرقمي.

المطلب الثاني: الإطار الإجرائي للحماية من المحتويات الاصطناعية غير التوافقية

لا يكفي وضع نصوص تجريم وعقوبات على الورق ما لم تواكبها آليات إجرائية فعالة لكشف الجريمة وضبط مرتكبيها وتقديمهم للعدالة. في حالة المحتويات الاصطناعية غير التوافقية، يواجه نظام العدالة الجنائية تحديات خاصة تتعلق بطبيعة هذه الجرائم الرقمية وعابرة للحدود وصعوبة اكتشافها تقنيا. وعليه، سوف نتناول في هذا المطلب جانبين يكمل أحدهما الآخر: أولًا وسائل الإثبات الجنائي والتحديات التقنية في التحقيق بقضايا المحتوى الاصطناعي غير التوافقي (الفرع الأول)، ثم دور الأجهزة القضائية والتنظيمية والتعاون الدولي في تتبع هذه الجرائم، نظرا للطابع العالمي للفضاء الإلكتروني (الفرع الثاني).

الفرع الأول: وسائل الإثبات وتحديات التحقيق الجنائي في الجرائم الرقمية الاصطناعية

تمثل جرائم التزييف العميق تحديا كبيرا لأجهزة إنفاذ القانون من حيث اكتشافها وإثباتها. فالمجرم هنا يستعين بالتكنولوجيا المتطورة لإخفاء فعلته أو لنقل يضفي على جريمته طابع "الواقعية" المزيفة، مما يجعل إثبات زيف المحتوى وتحديد الجاني مسؤولية تتطلب خبرات وأدوات فنية غير معتادة في التحقيقات الجنائية التقليدية. فيما يلي أبرز النقاط المتعلقة بوسائل الإثبات والتحديات في هذا المجال، مقرونة بما يتوافر في فرنسا والإمارات وربما العراق من إمكانيات:

اولا: اكتشاف المحتوى المزيف وتمييزه عن الحقيقي: أول عقبة تواجه المحققين هي الكشف التقني عما إذا كان المحتوى محل الشك مزيفًا فعلًا أم حقيقيا. فإذا أنكر شخص صحة فيديو منسوب له، على جهة التحقيق أن تثبت أن الفيديو مزيف (وذلك من جانبين: نفي نسبة الفعل للضحية وإثبات استخدام تقنية توليدية). تقنيا، هناك وسائل متطورة قيد التطوير لاكتشاف التزييف، مثل برمجيات تحليل الصور والفيديو التي تبحث عن شوائب رقمية تميز المحتوى المصطنع (كعدم الترابط في البكسلات عند تكبير الصورة، أو رصد انعكاسات غير طبيعية في العينين، أو اختلافات في معدل طرف العين مثلا، لأن بعض خوارزميات

التزييف تهمل هذه التفاصيل)[٣٧]. أيضا يمكن استخدام خوارزميات تعلم آلة مضادة مدربة على كشف التزييف، بحيث تفحص المقطع وتعطي احتمالية كونه مزيفا. إلا أن الخبراء يؤكدون أنه حتى هذه الكواشف ليست مضمونة ١٠٠٪ لأن المزورين يطورون تقنيات تتغلب عليها[٣٨]. وذكر مجلس الأمن السيبراني الإماراتي أن حتى الخبراء يمكن أن يصعب عليهم التفريق أحيانا بين المحتوى الحقيقي والمزيف لشدة دقته. لذلك عبء الإثبات هنا ثقيل؛ إذ قد يحتاج الادعاء العام في دولة كفرنسا إلى الاستعانة بخبير أو فريق خبراء رقميين لإجراء تحليل forensic للفيديو. وفي الإمارات، تمتلك الأجهزة الشرطية مثل شرطة دبي مختبرات رقمية متقدمة قد تساعد في تحليل المقاطع المشكوك فيها (فضلا عن إدخال منظومة ذكاء اصطناعي قادرة على التنبؤ بالجريمة وكشف الصور المزورة بدرجة عالية)[٣٩]. أما في العراق، فيكاد ينعدم وجود مختبرات جنائية رقمية متخصصة؛ ربما يتم اللجوء إلى أدلة ظرفية (كشهادة شهود على تواجد المتهم بمكان آخر وقت تصوير مزعوم، إلخ) أو إلى طلب مساعدة دولية من مختبرات أجنبية. وعليه، إحدى التوصيات المهمة هي بناء أو تحديث وحدات التحقيق الجنائي الرقمي وتجهيزها بأحدث أدوات اكتشاف التزييف.

ثانيا: تحديد هوية الجاني الرقمي: حتى لو ثبت أن الفيديو مزيف، يبقى التحدي الأهم من الذي صنعه أو نشره؟ فالجرائم الإلكترونية ترتكب غالبا تحت ستار أسماء مستعارة وحسابات وهمية، وقد يقوم الجاني باستخدام شبكات افتراضية خاصة (VPN) لإخفاء عنوانه، أو ينشر المادة عبر منصات أجنبية خارج ولاية سلطات بلده. في فرنسا، لدى الشرطة القضائية وحدات مختصة بالجرائم السيبرانية (OCLCTIC) يمكنها تتبع مصدر النشر عبر التعاون مع منصات التواصل لتزويدها بعنوان IP للجاني وقت النشر، ثم مخاطبة مزودي خدمة الإنترنت للوصول لبيانات المشترك صاحب ذلك الIP[٤٠]. هذه الإجراءات تخضع لإذن قضائي وخطوات رسمية لكنها متاحة. وفي حال كان المصدر خارج فرنسا، يتم التنسيق مع الإنتربول أو بالاستعانة بآليات المساعدة القانونية المتبادلة بين الدول[٤١]. اما في الإمارات، تملك السلطات صلاحيات موسعة للمراقبة الإلكترونية ورصد الأنشطة المشبوهة. وقد رأينا في المثال السابق كيف استطاعت شرطة دبي القبض على عصابة دولية للتزييف العميق المالي عبر جهود تحقيق عابرة للحدود. التعاون بين شرطة دبي وإنتربول فعال جدا، كما أن الإمارات طرف في اتفاقيات ثنائية ومتعددة لتسليم المجرمين. تستغل أيضا أنظمة الكاميرات والبصمات الحيوية؛ فلو نشر الجاني المحتوى من داخل الدولة، قد يتم كشفه عبر مراقبة كاميرات مقاهي الإنترنت أو أنظمة بصمة الوجه المنتشرة. أما في العراق، فالأمر أصعب بسبب ضعف البنية التقنية الأمنية. قد تلجأ السلطات إلى تعقب رقمي محدود عبر فرق الجرائم الإلكترونية في وزارة الداخلية، والتي تعتمد غالبا على تعقب حسابات التواصل من خلال المراسلة مع الشركات المالكة ,وربما تستعين بأجهزة الاستخبارات القادرة على إجراء اختراق تقني (وإن

كان ذلك خارج نطاق القانون أحيانا). من هنا تأتي أهمية انضمام العراق للاتفاقيات الدولية ليسهل الحصول على بيانات من شركات التواصل ومقدمي الخدمة الأجانب عند انتشار محتوى مزيف يطال مواطنيه.

ثالثا: جمع الأدلة الرقمية وحفظها: عندما يتم التعرف على الجاني المفترض، تحتاج السلطات إلى جمع الأدلة الإلكترونية بشكل يراعي الإجراءات القانونية وسلامة سلسلة الحفظ (Chain of Custody). مثلاً، يجب أن يتم توثيق المحتوى من الموقع الإلكتروني قبل حذفه (كطباعة الصفحة أو أخذ لقطة شاشة موقعة زمنيا)، وربما حفظ النسخة الرقمية الأصلية وفحص بياناتها الوصفية (Metadata) التي قد تكشف أشياء مثل برنامج التعديل المستخدم أو تاريخ الإنشاء الأصلي. كذلك عند ضبط حاسوب المتهم، يجب إجراء تفتيش إلكتروني قانوني للبحث عن ملفات المشروع أو صور المصدر الأصلية التي استخدمها في التركيب[٤٢]. في فرنسا والإمارات، تسمح قوانين الإجراءات الجنائية بالتفتيش الإلكتروني بموجب أمر قضائي، وبحضور خبراء لضمان عدم العبث. وتوجد بروتوكولات معيارية لتحرير محضر بالتفاصيل التقنية لكل خطوة لضمان قبول الأدلة أمام المحكمة. في العراق، لا يزال موضوع الأدلة الرقمية غير واضح بشكل كاف في قانون أصول المحاكمات الجزائية، لكن المحكمة الاتحادية قررت في أحد أحكامها قبول الرسائل الإلكترونية دليلا إذا اقترنت بتقارير فنية تثبت صدورها. لذا من المهم تحديث قوانين الإثبات الجزائي العراقي لتشمل الأدلة الرقمية وتنظم إجراءات جمعها وفحصها، وربما استحداث نص يضفي حجية على التقارير الفنية الدولية لو قدمت وفق الأصول

رابعا: التحدي الفني القانوني في مواجهة إنكار الجريمة: أحد التحديات المثيرة هو ما يسمى "دفاع التزييف العميق" (Deepfake Defense)، حيث قد ينكر المتهم نسبة الفعل إليه زاعما أن الدليل نفسه ملفق. مثلاً، لو ووجه شخص بفيديو على هاتفه يظهر أنه كان يحمل على الجهاز برمجيات التزييف أو ملفات المشروع، قد يدعي أن تلك الملفات دست إليه عبر قرصنة أو أنها نفسها مفبركة. هذا يستلزم من المحققين فحص احتمال القرصنة واستبعاده عبر تحليلات أمنية، وإقناع المحكمة بأن الأدلة سليمة. هناك أيضا مبدأ قرينة البراءة، فقد يستغله بعض الجناة إذ لا يمكن تقنيا الجزم ١٠٠٪ بزيف فيديو معين، فيبقى شك معقول يستفيد منه المتهم. لذلك ربما تحتاج الجهات القضائية إلى مزيج من الأدلة: فنية (تقرير خبير يؤكد بنسبة عالية أن الفيديو مزيف) ومادية (إثبات صلة المتهم بالحادث كتسجيل محادثات له يتفاخر بالفعل أو تحويلات مالية أو غيرها). هذا المزيج هو ما يعول عليه للحصول على إدانة راسخة[٤٣].

خامسا: الوقت عامل حاسم: سرعة التحرك في هذه القضايا مهمة جدا. فكلما طال الوقت، زاد انتشار المحتوى، وصعب جمع الأدلة (قد يُحذف تلقائيا بعد فترة أو يعمد المتهم لحذف الحسابات والملفات). لذا تنبهت بعض التشريعات لوضع إجراءات طوارئ رقمية. مثلاً، الاتحاد الأوروبي في لائحة الخدمات الرقمية

(DSA) يلزم المنصات بإجراءات سريعة لإزالة بعض المحتوى الضار خلال ٢٤ ساعة بطلب من السلطات. على الصعيد الإجرائي، قد تمنح سلطات مداهمة فورية في جرائم معينة بدون انتظار إجراءات طويلة إذا كان التأخير يهدد بضياع الأدلة[٤٤]. اما في الإمارات يجوز الدخول الفوري لنظم المعلومات لوقف فعل مجرم أو لحفظ أدلة مهددة بالضياع، بإذن النيابة[٤٥]. في العراق، ربما يحتاج المشرع لإضافة مادة تتيح للجهات التحقيقية إصدار أوامر عاجلة لشركات الإنترنت للحفاظ السريع على البيانات الإلكترونية قبل الحصول على أمر بالتسليم، منعا لقيام الفاعل بحذفها.

بناء على ما سبق، نجد أن وسائل الإثبات في جرائم المحتوى الاصطناعي تتطلب توليفة من المعرفة التقنية والأدوات المتطورة والتنسيق مع الخبراء، إلى جانب تكييف الإجراءات القانونية لتلائم طبيعة الدليل الرقمي السريع الزوال. لقد بدأت دول متقدمة كفرنسا بالفعل في تزويد أجهزة الشرطة والقضاء بالأدوات اللازمة وتعزيز التعاون مع شركات التقنية لتسهيل الحصول على الأدلة. وفي الإمارات، قطعت الأجهزة الأمنية شوطًا ملحوظًا في بناء خبرات داخلية تسمح بكشف وتحليل هذه الجرائم كما ظهر في نجاحات ضبطها. أما العراق، فيحتاج إلى الاستثمار في بناء القدرات عبر تدريب فرق متخصصة في الأدلة الرقمية والتزييف الرقمي، وإيجاد قنوات اتصال مع مزودي الخدمات العالمية (مثل اتفاقات تعاون بين وزارة الداخلية العراقية ومنصات التواصل). كما يبرز ضرورة انضمام العراق إلى الاتفاقيات الدولية ذات الصلة (مثل اتفاقية بودابست للجرائم الإلكترونية) لتسهيل إجراءات التحقيق عبر الحدود. ذلك أن الجرائم السيبرانية لا تعترف بالحدود، وبالتالي الأدلة والشهود غالبا ما يكونون موزعين في دول شتى. بالتالي، يظل التعاون الدولي — الذي سنعالجه في الفرع التالي — عنصرا مكملاً لجهود التحقيق المحلية لضمان فعالية الملاحقة الجنائية في هذا المجال المعقد.

الفرع الثاني: دور الجهات القضائية والتنظيمية في ملاحقة الجناة والتعاون الدولي

في مواجهة الجرائم المستحدثة كتزييف المحتوى، لا يقتصر الأمر على دور الشرطة أو أجهزة التحقيق الجنائي فقط، بل يمتد إلى منظومة عدالة وجهاز قضائي متخصص قادر على فهم أبعاد هذه القضايا وإدارتها بفعالية. كما أن التنظيم الإداري والهيئات الرقابية تلعب دورا وقائيا هاما، بالتوازي مع التعاون الدولي الذي أصبح حجر الزاوية في مكافحة الجرائم الإلكترونية التي تتجاوز حدود أي دولة منفردة. في هذا الفرع نتناول ثلاثة محاور: اولا تأهيل الجهات القضائية (قضاة ونيابة) للتعامل مع جرائم المحتوى الاصطناعي؛ وثانيا دور الهيئات التنظيمية والرقابية المحلية في الحد من انتشار المحتوى المجرم؛ واخيرا آليات التعاون الدولي بين فرنسا والإمارات والعراق وغيرها في مجال مكافحة التزييف العميق.

اولا: تأهيل وجهوزية الجهات القضائية (القضاة والنيابات المتخصصة):

التعامل مع قضية تتعلق بمقطع Deepfake يتطلب من القاضي أو عضو النيابة فهما لطبيعة التقنية واحتمالات الخطأ والصواب فيها. ومن هنا بدأ الاتجاه نحو تدريب قضائي متخصص. في فرنسا، هناك توجه لإنشاء وحدات نيابة عامة متخصصة بالجرائم الرقمية (كما يوجد للجرائم

https://doi.org/10.61353/ma.0210133

المالية والإرهابية)، بحيث يتولى تلك القضايا وكلاء نيابة متمرسون في المسائل التقنية ولديهم خبراء استشاريون. كما تنظم دورات للقضاة حول الأدلة الرقمية وكيفية تقييم تقارير الخبرة الفنية. ومن الجدير ذكره أن القاضي الفرنسي يتمتع بصلاحية واسعة في تعيين خبير أو لجنة خبراء متى ما استلزم الأمر في مسائل تقنية معقدة، فيستطيع مثلاً طلب رأي خبير معتمد في تكنولوجيا المعلومات لتأكيد ما إذا كان فيديو معين مزيفاً. كذلك يمكن للقاضي أن يأمر بجلسات سرية لحماية خصوصية الضحية إذا كان الفيديو إباحيا، ويمنع تداول محتوى القضية خارج المحكمة[٤٦].

في الإمارات، أنشأت في دبي نيابات تقنية ضمن نيابة جرائم تقنية المعلومات، بحيث تُحال إليها قضايا الابتزاز الإلكتروني والتشهير عبر الإنترنت. وهؤلاء أعضاء النيابة تلقوا تدريبات على ملاحقة هذا النوع من الجرائم. كما أن المعهد القضائي الإماراتي يعقد ورش عمل حول الجرائم الإلكترونية للمستشارين والقضاة الجدد. أيضا تصدر المحاكم الإماراتية أحكاما رادعة وسريعة في هذه القضايا، مما يدل على فعالية الإعداد. مثلاً، في إحدى قضايا الابتزاز الجنسي بواسطة صور مزيفة صدرت أحكام بالحبس لعدة سنوات على الجناة في زمن قياسي، مما يعطي رسالة أن القضاء مواكب ويبعث الطمأنينة للضحايا[٤٧].

أما في العراق، فالوضع بحاجة إلى تطوير. فحتى الآن لا توجد محاكم أو هيئات تحقيق متخصصة بجرائم تقنية المعلومات (ما عدا تجربة في إقليم كردستان حيث شكلت مديرية للجرائم الإلكترونية). غالبا ما تُحال قضايا التشهير الإلكتروني إلى محاكم التحقيق العادية، وقد يواجه القاضي صعوبة في فهم طريقة نشر المحتوى أو تتبع الحسابات. هناك ضرورة لإنشاء محاكم/هيئات تحقيق متخصصة بالجرائم الإلكترونية تضم قضاة وضباط تحقيق تلقوا تدريبا تقنيا أساسيا، أو على الأقل تعيين خبراء تقنيين لمعاونة القضاء في هذه الدعاوى. ويجدر بمجلس القضاء الأعلى العراقي التعاون مع منظمات دولية أو مع دول مثل فرنسا والإمارات لتنظيم دورات تدريبية أو زيارات اطلاع للقضاة وأعضاء الادعاء العام لاكتساب الخبرات في التعامل مع هذا النوع المستحدث من الجرائم.

ثانيا: دور الجهات التنظيمية والهيئات غير القضائية محليًا:

الجهات التنظيمية قد تشمل هيئات الإعلام والاتصالات، هيئات حماية البيانات الشخصية، المؤسسات الأمنية ذات الطابع الوقائي. دور هذه الجهات مهم في منع أو تقليل انتشار المحتوى الضار قبل الوصول لمرحلة التقاضي.

في فرنسا، يلعب المجلس الأعلى للإعلام السمعي البصري (CSA) دورا في مراقبة منصات التواصل من خلال مطالبة الشركات باتخاذ خطوات لمنع التزييف الضار. أيضا لدى فرنسا هيئة لحماية البيانات (CNIL) يمكن أن تتدخل إذا تضمن الأمر معالجة غير قانونية لبيانات شخصية (مثل استخدام صور شخص دون إذنه

قد يخالف قانون حماية البيانات). فرنسا أيضا ضغطت على الشركات ضمن الاتحاد الأوروبي لتطوير مدونات سلوك تتعلق بالتزييف العميق، مثل التزام شركات التواصل الاجتماعي بتعقب وإزالة المقاطع المضللة سياسيا بسرعة[٤٨].

أما في الإمارات، مجلس الأمن السيبراني الذي صدر تحذيره الرسمي الأخير حول مخاطر التزييف العميق هو مثال لجهة تنظيمية توعوية. كذلك تلعب هيئة تنظيم الاتصالات دورا في حجب المواقع بالتنسيق مع شركات الاتصالات المحلية عند الضرورة. الإمارات أيضا لديها إدارة في وزارة الداخلية لمكافحة الجرائم الإلكترونية تقوم برصد المحتوى المشتبه به على الانترنت (وتتلقى بلاغات على الخط الساخن) وتعمل بشكل استباقي أحيانا بإبلاغ المنصات لإزالة محتوى أو إغلاق حسابات. علاوة على ذلك، اتفقت الإمارات مع شركات مثل فيسبوك ويوتيوب على آليات سريعة للإبلاغ عن المحتوى غير القانوني ليتم حذفه وفق سياسات تلك الشركات[٤٩].

وفي العراق، يوجد هيئة الإعلام والاتصالات (CMC) والتي لها صلاحيات على مزودي خدمات الانترنت والإعلام. لكنها تعاني أحيانا من قيود وإرباك في الصلاحيات. لم نسمع عن دور نشط لها في ملاحقة المحتوى الإلكتروني الضار إلا في إطار الرقابة على المحتوى السياسي والإعلامي. ينبغي تعزيز دورها ليشمل متابعة المحتوى المزيَّف والمسيء، بحيث تمتلك وحدة ترصد منصات التواصل وتبلغ الشرطة عن أي محتوى يتضمن تركيبا مسيئا لأحد الأشخاص، خاصة المحتوى الذي يمكن أن يهدد السلم المجتمعي (كالفيديوهات المفبركة ذات الطابع الطائفي أو التحريضي). كما يمكن للهيئة بالتعاون مع وزارة الداخلية إنشاء خط ساخن مختص ببلاغات ضحايا التزييف العميق، مما يشجع المتضررين على سرعة الإبلاغ بدل الشعور بالعجز.

بوجه عام، التوعية هي جزء من الوقاية التنظيمية. نشر مجلس الإمارات للأمن السيبراني بيانات تحذيرية هو مثال جيد. أيضا قيام الإعلام بحملات توعوية عن خطورة تداول المقاطع دون التحقق وسرد قصص الضحايا (مع الحفاظ على خصوصيتهم) يمكن أن يرفع وعي الجمهور. هذا بدوره يقلل تأثير المحتوى المزيف لأن الناس سيصبحون أكثر تشككًا ويعرفون كيف يميزون أو يبلغون الجهات المختصة.

ثالثا: التعاون الدولي لملاحقة جرائم المحتوى الاصطناعي غير التوافقي:

كما كررنا، هذه الجرائم عابرة للحدود بطبيعتها. فالجاني يمكن أن يكون في دولة والضحية في دولة ثانية والمحتوى مستضاف على خوادم دولة ثالثة. لذا بدون تعاون دولي، قد يتمتع الكثير من الجناة بالإفلات. هنا تلعب الاتفاقيات والمؤسسات الدولية دورا كبيرا:

١. الإنتربول والمنظمات الشرطية الدولية: أصبح لدى الإنتربول في السنوات الأخيرة مبادرات خاصة بالجرائم السيبرانية. ففي ٢٠٢٠ أطلق الإنتربول مشروعا بعنوان "ما بعد الأوهام – Beyond Illusions" يسعى لفهم واستحداث طرائق لكشف استخدامات التزييف العميق في الجريمة. كما

https://doi.org/10.61353/ma.0210133

ينظم الإنتربول تدريبات مشتركة لضباط من دول مختلفة على أدوات كشف التزييف[٥٠]. والأهم، أنه يوفر قناة تواصل آمنة بين أجهزة الشرطة لتبادل المعلومات سريعا عن مثل هذه الجرائم. على سبيل المثال، إذا كان هناك مشتبه في فرنسا ينشر مواد تزييف تستهدف شخصا في الإمارات، يمكن عبر مكتب الإنتربول في أبوظبي طلب تتبع وتحقيق من المكتب في باريس. وقد حصل تعاون فعلي في قضايا احتيال Deepfake مالي ضبط فيها العشرات عبر تنسيق دولي. كذلك أعلنت الإنتربول عام ٢٠٢٣ توقيف ٣,٥٠٠ شخص حول العالم في جرائم احتيال عبر deepfakes ورومانسية، وضبط ١٠٠ دولة أموالاً وأصولاً خلال عملية مشتركة، مما يدل على تنامي قدرة الإنتربول على حشد الجهود ضد هذا التهديد الجديد[٥١].

٢. الاتفاقيات القضائية الثنائية والمتعددة: فرنسا كجزء من الاتحاد الأوروبي تستفيد من أدوات أوروبية مثل أوامر التحقيق الأوروبية التي تسمح للادعاء الفرنسي بطلب أدلة من خوادم أو شركات في دول أوروبية أخرى بسرعة نسبية. كما أن فرنسا موقعة على اتفاقية بودابست للجرائم الإلكترونية ٢٠٠١، التي تعد الإطار الدولي الرئيسي للتعاون في مجال الجرائم المعلوماتية. هذه الاتفاقية (انضمت لها أكثر من ٦٥ دولة) تضع آليات لطلبات المساعدة القانونية وتسليم المجرمين في الجرائم السيبرانية[٥٢]. الإمارات في المقابل ليست طرفاً في اتفاقية بودابست، لكنها عقدت مذكرات تفاهم ثنائية مع دول كثيرة للتعاون في مكافحة الجرائم التقنية. كما أنها عضو فاعل في المنتدى العالمي للأمن السيبراني. إضافة لذلك، دولة الإمارات أصبحت من الدول السباقة في طرح قضايا الجرائم الإلكترونية في المنظمات الدولية (مثل الأمم المتحدة) وتدعو لوضع "مدونة سلوك دولية" لتقنين استخدامات الذكاء الاصطناعي على المستوى العالمي. أما العراق فلا يزال خارج أغلب الأطر الدولية المنظمة للجرائم السيبرانية (فلم ينضم إلى اتفاقية بودابست حتى الآن)، مما يحدّ من قدرته على ملاحقة الجناة عبر الحدود. ومن هنا تتضح ضرورة تفعيل التعاون الدولي عبر قنوات متعددة: انضمام العراق مستقبلاً إلى اتفاقيات الجرائم الإلكترونية؛ تعزيز التعاون الأمني مع دول الجوار والإنتربول؛ والاستفادة من خبرات الدول الرائدة (مثل فرنسا والإمارات) بتوقيع مذكرات تفاهم لتبادل المعلومات والتدريب في مجال مكافحة المحتوى الاصطناعي غير التوافقي. كما يمكن للعراق طلب الدعم الفني من هيئات دولية (كالمكتب الدولي لمكافحة المخدرات والجريمة التابع للأمم المتحدة UNODC) لتطوير قدراته التشريعية والتحقيقية في هذا الميدان.

وخلاصة الأمر، أن تكاتف الجهات القضائية والتنظيمية الوطنية مع الجهود الدولية هو السبيل الناجع لملاحقة جرائم المحتويات الاصطناعية غير التوافقية. فقد بينت التجربة الفرنسية أهمية وجود إطار قانوني حديث وواضح يعمل القضاة في ظلّه، بينما أبرزت التجربة الإماراتية جدوى وجود فرق شرطية متخصصة مدعومة

بتشريعات مرنة للتصرف السريع. أما العراق، فعليه الاستفادة من هذين النموذجين عبر تحديث تشريعه وبناء قدراته والتعاون مع المجتمع الدولي حتى لا يصبح حلقة أضعف يستغلها المجرمون لكونها خارج المنظومة العالمية لمكافحة هذا النوع من الجرائم.

الخاتمة

تمخض البحث عبر صفحاته السابقة عن دراسة معمقة لظاهرة المحتويات الاصطناعية غير التوافقية ومخاطرها الجسيمة، وتحليل كيفية مواجهة ثلاث دول لها من زاوية القانون الجنائي المقارن. ومن خلال هذه الدراسة، يمكن استخلاص جملة من الاستنتاجات والمقترحات:

أولًا: الاستنتاجات:

١- أثبتت الدراسة أن المحتويات الاصطناعية غير التوافقية تمثل نمطًا مستحدثًا من الإجرام الرقمي يعتدي في آن واحد على أمن المجتمع الرقمي (بنشر الخداع والاحتيال وزعزعة الثقة العامة) وعلى حقوق الأفراد الأساسية في الخصوصية والسمعة. وهي ظاهرة مرشحة للازدياد مع تطور تقنيات الذكاء الاصطناعي، ما لم يتم تطويقها بتشريعات وإجراءات صارمة.

٢- كشف البحث تفاوتا واضحا في تعاطي النظم القانونية محل الدراسة مع هذه الظاهرة, فقد بادر المشرع الفرنسي إلى سد الفراغ التشريعي عبر تعديل قانون العقوبات (عام ٢٠٢٤) لتجريم صريح لفعل نشر المحتوى الاصطناعي غير التوافقي، مع استحداث نص خاص بالمحتوى الجنسي المزيف. وجاءت العقوبات الفرنسية متدرجة (حتى ١-٢ سنة حبس في الحالات العادية، ترتفع إلى ٢-٣ سنوات في الحالات المشددة كالإباحية أو استخدام الإنترنت)، مما يؤكد جدية المشرع في الردع دون إفراط. في المقابل، يعتمد القانون الإماراتي على منظومة جرائم قائمة (كالتشهير الإلكتروني، وانتهاك الخصوصية، والاحتيال الإلكتروني، ونشر الشائعات) لتجريم أفعال المحتوى الاصطناعي غير التوافقي. ورغم عدم ذكر "المحتويات الاصطناعية غير التوافقية" صراحة في المواد، إلا أن النصوص مرنة وواسعة بحيث تغطي معظم صور السلوك المجرم. وتمتاز الإمارات بعقوبات صارمة نسبيا لاسيما من ناحية الغرامات الضخمة (ربع إلى نصف مليون درهم للتشهير مثلًا)، وبإجراءات خاصة كحجب المواقع، مما يشكل رادعا فعالًا.

٣- اتضح أن القانون العراقي الحالي يعاني قصورا تشريعيا في مواجهة هذه الظاهرة. فلا توجد نصوص جنائية حديثة تعالج المحتويات الاصطناعية غير التوافقية ، ويضطر القضاء إلى تكييف الأفعال ضمن جرائم تقليدية (كالقذف والسب) بعقوبات متواضعة نسبيا (حبس سنة أو أقل). وهذا قد يؤدي إلى إفلات بعض الأفعال الخطيرة من العقاب أو معاقبتها بأقل مما تستحق، فضلًا عن إشكاليات مبدأ الشرعية إذا تم التوسع كثيرا في التكييف. وبالتالي يتأكد وجود فراغ تشريعي في القانون العراقي بخصوص التجريم المحدد للمحتويات الاصطناعية غير التوافقية.

https://doi.org/10.61353/ma.0210133

٤- على صعيد الإجراءات الجنائية، برهنت التجربة العملية أن التحقيق في هذه الجرائم يتطلب تجهيزات تقنية عالية ومهارات خاصة. وقد أظهرت فرنسا والإمارات تقدما في هذا المجال عبر إنشاء وحدات شرطية متخصصة واستخدام خبراء وتقنيات لكشفها. بينما لا يزال العراق بحاجة إلى تطوير قدراته الفنية في جمع الأدلة الرقمية وتحليلها، وإلى تحديث تشريعات الإجراءات لإدخال الأدلة الإلكترونية ومعاونات التحقيق الدولي بصورة أكثر فعالية.

٥- بين البحث كذلك أن التعاون الدولي بات عنصرا حاسما: حيث استفادت فرنسا من إطار التعاون الأوروبي واتفاقية بودابست، واستفادت الإمارات من شراكاتها الدولية وعضويتها الفاعلة في الإنتربول، مما سهل ملاحقة الجناة عبر الحدود. أما العراق فيعاني من ضعف الارتباط بتلك الأطر، مما يفرض عليه الإسراع بالانخراط في المنظومة الدولية لمكافحة الجرائم السيبرانية كي لا يصبح ملاذاً آمناً لمجرمي المحتوى الاصطناعي غير التوافقي.

٦- من زاوية حماية الضحايا، ظهر أن القانون الفرنسي والإماراتي يتضمنان أدوات جيدة نسبيا (كإمكانية الأمر بإزالة المحتوى سريعا، وحماية خصوصية الضحية في المحاكمة، وحقها في التعويض)، بينما الوضع في العراق أقل ضماناً لحقوق الضحية سواء في سرعة إزالة المحتوى أو في اقتضاء تعويض ملائم. وهذا يستدعي تبني إجراءات مساندة في التشريع العراقي لضمان إزالة المحتوى الضار فورا وتخفيف الضرر عن الضحايا.

ثانيًا: المقترحات:

بناء على ما تقدم من استنتاجات، نطرح فيما يأتي عددا من المقترحات لتعزيز الحماية الجنائية من المحتويات الاصطناعية غير التوافقية، خاصة في البيئة القانونية العراقية التي تحتاج لتحديث في هذا الصدد:

١. تعريف وتجريم المحتوى الاصطناعي غير التوافقي (مع استثناء للمحتوى الساخر أو الفني): ينبغي للمشرع العراقي إما إدراج مادة جديدة في قانون العقوبات أو في قانون الجرائم المعلوماتية المقترح، تعرف "المحتوى الاصطناعي غير التوافقي" بشكل واضح ، وتجرم بشكل صريح فعل إنشاء أو نشر أو تداول هذا المحتوى. من خلال الإفادة من التجربة الفرنسية في المادة ٢٢٦-٨ إذ يغطي التجريم أي صورة أو تسجيل مولّد حاسوبيا يمثل شخصا بدون رضاه مع اعتبار عدم الإفصاح عن زيفه قرينة على نية الخداع. و أن تتضمن المادة استثناء صريحا لما يكون محتوى فنياً أو ساخراً مع الإفصاح الواضح عن ذلك وذلك للحفاظ على هامش الإبداع وحسن النية. والنص المقترح لهذه المادة: " يعاقب بالحبس مدة لا تزيد على سنة واحدة وبغرامة لا تزيد على عشرة ملايين دينار, كل من قام بإنتاج أو إنشاء أو ترويج أو نشر، بأي وسيلة كانت، لمحتوى اصطناعي غير توافقي يتضمن صورة شخص أو صوته أو كليهما، ويقصد بالمحتوى الاصطناعي غير التوافقي أي تركيب رقمي أو معالجة

خوارزمية تولّد مظهراً أو صوتاً لشخص على نحو يوهم بأنه حقيقي دون رضاه. ويستثنى من التجريم المحتوى الذيَ يكون من الواضح لدى الشخص العادي أنه تركيب أو عمل فني أو ساخر، أو الذي يصرَّح بشكل جلي بأنه محتوى مصطنع."

٢. تشديد العقوبة في حالة المحتوى ذو الطبيعة الجنسية أو المستخدم للابتزاز او اذا كانت الضحية حدثا او اذا تم النشر على نطاق واسع عبر الإنترنت: نقترح بأن يتضمن القانون العراقي نصا يعاقب بشدة على إنشاء أو نشر صور أو مقاطع ذات طبيعة جنسية أو إباحية لشخص (سواء حقيقية أو مزيفة بتقنيات رقمية) دون رضاه. كذلك إضافة ظرف مشدد إذا كان الضحية قاصرا أو أن النشر كان على نطاق واسع عبر الإنترنت. والنص المقترح لهذه المادة : " : إذا كان المحتوى الاصطناعي غير التوافقي المشار إليه في المادة السابقة ذا طبيعة جنسية فاضحة، أو كان الهدف من إنتاجه أو نشره ابتزاز الشخص الضحية أو إكراهه، فتكون العقوبة الحبس مدة لا تزيد على ثلاث سنوات وبغرامة لا تزيد على عشرين مليون دينار. وتَعد من الظروف المشددة ما إذا كان الشخص الضحية حدثاً أو إذا تم توزيع المحتوى على نطاق واسع باستخدام شبكة المعلومات أو وسائل التواصل الاجتماعي؛ وفي هذه الحالات يجوز أن تصل العقوبة إلى الحبس لمدة لا تزيد على خمس سنوات والغرامة إلى خمس وعشرين مليون دينار."

٣. مقترح بخصوص عقوبات جرائم القذف والتشهير العلني : نقترح ان يكون النص في حالات القذف او التشهير الاتي : " مع عدم الإخلال بأية عقوبة أشد ينص عليها القانون، لا تقل عقوبة الحبس والغرامة المنصوص عليها في المواد أعلاه عن العقوبة المقررة لجرائم القذف أو التشهير العلني المنصوص عليها في هذا القانون. وفي جميع الأحوال، يجوز للمحكمة الحكم بغرامة تصل إلى ضعف الحد الأقصى المقرر لجرائم التشهير التقليدية إذا ارتَكبت الأفعال المجرَّمة بموجب المواد أعلاه بقصد التشهير أو الإضرار بسمعة المجني عليه."

٤. تجريم الأفعال المساعدة أو اللاحقة (مثل تسليم المحتوى أو إعادة نشره بقصد الإضرار): فبالنظر لطبيعة هذه الجرائم، قد لا يقتصر الفعل على شخص واحد (المنشئ الأصلي للمحتوى)، بل قد يتورط آخرون في نشره أو إعادة إرساله بقصد الإضرار بالضحية أو دعم الجاني الأصلي. لذا من المهم سد أي ثغرة يمكن أن يستغلها المتواطئون بحجة أنهم لم يصنعوا المحتوى بل فقط تداولوه؛ فإذا علم الناس أن مجرد إعادة التغريد لمادة مزيفة مسيئة يمكن أن يوقعهم تحت طائلة القانون إذا ثبت علمهم، سيكونون أكثر حذرا. والنص المقترح لهذه المادة : " يعاقب بالعقوبة ذاتها المنصوص عليها للجريمة الأصلية كل من قام، بقصد تسهيل ارتكاب أي من الجرائم المنصوص عليها في المواد أعلاه أو الإسهام في آثارها الضارة، بتسليم المحتوى الاصطناعي غير التوافقي أو توفيره للغير أو إعادة نشره

https://doi.org/10.61353/ma.0210133

أو تداوله بأي صورة كانت مع علمه بطبيعته غير الحقيقية وبأنه غير توافقي. كما تطبق العقوبات ذاتها على من يساعد بأي شكل في توزيع ذلك المحتوى أو إخفائه أو إتلاف الأدلة المتعلقة به بقصد تمكين الجاني من الإفلات من العقاب."

٥. استحداث آلية قضائية عاجلة لحذف المحتوى المسيء من المنصات: نقترح تضمين نص يتيح للمتضرر أو الادعاء العام استصدار أمر قضائي عاجل يلزم الجهة المستضيفة (الموقع أو المنصة) بحذف المحتوى المسيء فورا أو خلال مدة قصيرة، تحت طائلة غرامة تهديدية. وربما التنسيق مع الشركات المالكة للمنصات عبر مذكرات تفاهم لتسهيل الإجراءات (على غرار تعاون السلطات مع فيسبوك في قضايا الإرهاب مثلا). إن سرعة الإزالة تحدّ كثيرا من تفاقم الضرر، لذا يجب تقنينها كجزء من الحماية الجنائية. يمكن للمحكمة أيضا عند البت في القضية أن تقضي ضمن حكمها النهائي بإلزام الجاني أو المنصة بنشر اعتذار أو تصحيح لتوضيح زيف المحتوى ورد الاعتبار للضحية. والنص المقترح لهذه المادة : " للمحكمة المختصة أو قاضي الأمور المستعجلة أن يصدر، بناء على طلب المتضرر أو الادعاء العام، أمرا قضائيا واجب النفاذ على وجه السرعة بحذف أو حجب المحتوى الاصطناعي غير التوافقي المجرم بموجب المواد أعلاه، سواء من موقع إلكتروني أو منصة رقمية أو أي وسيلة نشر أخرى، متى كان وجود ذلك المحتوى قابلاً للاستمرار في إلحاق الضرر بالضحية. وعلى الجهة أو الشخص المعني بحيازة المحتوى أو استضافته أو نشره تنفيذ الأمر القضائي فور صدوره، وإلا تعرض للعقوبات المقررة قانونا للامتناع عن تنفيذ الأوامر القضائية."

٦. دعم التحقيقات الرقمية عبر وحدة متخصصة واعتماد وسائل الإثبات التقنية: نقترح تضمين نص لتزويد أجهزة التحقيق الجنائي في العراق بأدوات تقنية وخبراء قادرين على اكتشاف التزييف العميق وتمييزه. فنجاح المقاضاة يعتمد على إثبات أن المحتوى مزيف وتحديد هوية من صنعه. كما نقترح تأسيس وحدة متخصصة من ضمن الأدلة الجنائية الرقمية تعنى بتحليل المقاطع والصور لكشف أي تلاعب خوارزمي، وربط ذلك بالأجهزة أو الحسابات المستخدمة من قبل الجناة. كما ينصح بتدريب القضاة وأعضاء الإدعاء العام على فهم أساسيات التقنية وتقدير خطورة هذه الأفعال، حتى يتعاملوا بجدية ووعي مع القضايا المعروضة. والنص المقترح لهذه المادة : " على الجهات المختصة بالتحقيق والتحري (ومنها وزارة الداخلية والأجهزة الأمنية الفنية) إنشاء أو تخصيص وحدة فنية متخصصة في جرائم التقنيات الحديثة، تزود بالخبراء والتجهيزات اللازمة لكشف أدلة الجرائم المعلوماتية ومنها جرائم المحتوى الاصطناعي غير التوافقي. وتعد التقارير الفنية الصادرة عن هذه الوحدة أو عن خبراء تقنيين معتمدين بمثابة أدلة إثبات مشروعة أمام المحاكم، ويجوز للقاضي الأخذ بها فيما يتعلق بإثبات كون

المحتوى محل الاتهام قد جرى توليده أو تعديله رقمياً أو تحديد هوية المنشئ أو الناشر الأصلي أو غير ذلك من الأمور الفنية."

٧. تضمين واجب التوعية العامة من ضمن مسؤوليات الجهات الرقابية والمؤسسات الإعلامية: أخيرا، نقترح تضمين نص لإطلاق حملات مشتركة بين الجهات القانونية والتقنية للتوعية بمخاطر التزييف العميق. على غرار تحذير مجلس الأمن السيبراني الإماراتي، يمكن لوزارة الداخلية العراقية أو هيئة الإعلام والاتصالات إصدار بيانات رسمية تؤكد أن صنع أو نشر صور مزيفة لأشخاص هو فعل جرمي يعاقب عليه القانون، وتشجع الضحايا على الإبلاغ فورا. كما يمكن التعاون مع مؤسسات المجتمع المدني لنشر ثقافة "لا تصدق كل ما تراه" وحث المستخدمين على التحقق من مقاطع مثيرة قبل إعادة نشرها. فالمجتمع الواعي هو خط الدفاع الأول ضد التضليل. والنص المقترح لهذه المادة : " يلتزم الجهات ذات العلاقة بالرقابة على الفضاء الإلكتروني والإعلام (ومنها هيئة الإعلام والاتصالات ووزارة الداخلية والمؤسسات الإعلامية الحكومية والخاصة) باتخاذ التدابير اللازمة لنشر الوعي العام بمخاطر إساءة استخدام تقنيات الذكاء الاصطناعي في إنتاج المحتوى الزائف (المحتوى الاصطناعي غير التوافقي)، وسبل التعرف عليه والإبلاغ عنه للسلطات المختصة. ويتم ذلك من خلال حملات إعلامية وتثقيفية دورية في وسائل الإعلام والمنصات الرقمية والتنسيق مع المؤسسات التعليمية لنشر ثقافة الاستخدام الآمن للتكنولوجيا والتحقق من صحة المحتويات الرقمية."

المصادر:

[١] ينظر:
Sarah A. Fisher, Jeffrey W. Howard, and Beatriz Kira, "Moderating Synthetic Content: the Challenge of Generative AI," *Philosophy & Technology* 37, no. 4 (November 13, 2024): 133, p.1-20.

[٢] ينظر:
Simon Robichaud-Durand, " L'hypertrucage : analyse du phénomène des « deepfakes » et recommandations , *Lex Electronica* 28, Lex Electronica,Volume 28,(Number 4, 2023), p. 78–98.

[٣] ينظر : Ibid.

[٤] ينظر :
Mihaela Mihailova, "In Focus Introduction: AI and the Moving Image," *JCMS: Journal of Cinema and Media Studies* 64, no. 1 (2024), p.170.

[٥] ينظر :
"LOI N° 2024-449 Du 21 Mai 2024 Visant à Sécuriser et à Réguler l'espace Numérique (SREN), Modifiant Notamment l'article 226-8 Du Code Pénal Concernant Les Contenus Audiovisuels Générés Artificiellement sans Consentement Explicite." (2024).

[٦] ينظر :
Robert Chesney and Danielle Keats Citron, "Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security," *SSRN Electronic Journal*, 2018,.p.1763.

https://doi.org/10.61353/ma.0210133

[٧] ينظر : . Ibid

[٨] ينظر :

Henry Ajder et al., "The State of Deepfakes: Landscape, Threats, and Impact" Deeptrace (2019),p. 1.

[٩] في عام ٢٠١٨ ,اظهرت مقاطع مزيفة للرئيس الأمريكي السابق أوباما وهو يدلي بتصريحات مسيئة تعبّر بدقة عن نبرة صوته وحركات وجهه. هذه الأمثلة أظهرت أن التزييف العميق تجاوز حدود المواد الإباحية ليشمل شخصيات سياسية وعامة ضمن محتويات ساخرة أو مضللة، مما وسّع دائرة القلق من تبعاته, ينظر:

Todd C. Helmus, "Artificial Intelligence, Deepfakes, and Disinformation: A Primer" (RAND Corporation, 2022), https://doi.org/10.7249/PEA1043-1.

[١٠] ينظر :

Aaron Holmes, "Facebook Just Banned Deepfakes, but the Policy Has Loopholes — and a Widely Circulated Deepfake of Mark Zuckerberg Is Allowed to Stay Up," Business Insider, June 7, 2019, https://www.businessinsider.com/facebook-just-banned-deepfakes-but-the-policy-has-loopholes-2020-1. last access 1-4-2025.

[١١] ينظر:

Robert Chesney and Citron, "Deep Fakes" Op.cit., p.1753.

[١٢] ينظر:

European Union, "Proposal for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative" (2021), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0206.

[١٣] ينظر:

Nmesoma Nnamdi, O.A. Oniyinde, and Babalola Abegunde, "An Appraisal of the Implications of Deep Fakes: The Need for Urgent International Legislations," *American Journal of Leadership and Governance* 8, no. 1, July 23, 2023, p.58.

[١٤] ينظر :

Catherine Stupp. "Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case." *Wall Street Journal*, August 30, 2019, sec. WSJ Pro. https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402.

[١٥] ينظر:

Ali Al Hammadi Reporter, "Watch: New Alert over Sharing Deep Fake Content in UAE," Gulf News: Latest UAE news, Dubai news, Business, travel news, Dubai Gold rate, prayer time, cinema, September 14, 2024, https://gulfnews.com/uae/crime/watch-new-alert-over-sharing-deep-fake-content-in-uae-1.104100475.

[١٦] لمزيد من التفاصيل, ينظر : دبار محمد أمين، وبابو جمال الدين، "تداعيات الذكاء الاصطناعي على الأمن القومي"، مجلة القانون الخاص، المجلد ٢، العدد ١ (١٧ يونيو ٢٠٢٤) : ص ١٠٠–١٢٢.

[١٧] لمزيد من التفاصل, ينظر : محمد السعيد عبد المولى، "الأثر السلبي لتطور الذكاء الاصطناعي على حجية الدليل الإلكتروني في المسائل الجزائية"، *حُماة الحق – محامي الأردن*، 26ديسمبر ٢٠٢٣، تم الدخول في ٨ أبريل ٢٠٢٥، https://jordan-lawyer.com/2023/12/26/الأثر-السلبي-لتطور-الذكاء-الاصطناعي-ع/.

[١٨] لمزيد من التفاصيل, ينظر : منة الله كمال موسى دياب، "سلوكُ حمايةِ الخصوصيَّةِ الرَّقميَّةِ البيومترية لدى مُستخدمي تطبيقاتِ التزييفِ العميقِ من طلبةِ الجامعاتِ المصريَّةِ"، المجلة العربية لبحوث الإعلام والاتصال، العدد ٣٧ (يونيو ٢٠٢٢): ص ١٨٤–٢٣٩

[١٩] لمزيد من التفاصيل : ينظر: أحمد المعداوي، "حماية الخصوصية المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي"، مجلة كلية الشريعة والقانون – جامعة الأزهر، العدد الثالث والثلاثون – الجزء الرابع. ٢٠١٨

[٢٠] ينظر: مجلس الإشراف على ميتا، "صور فاضحة بالذكاء الاصطناعي لشخصيات عامة نسائية"، ٢٠٢٤، تم الاطلاع عليه في ٨ أبريل ٢٠٢٥، https://www.oversightboard.com/decision/bun-7e941o1n/?lang=ar.

[٢١] ينظر:

Julie Posetti and Nabeelah Shabbir, *A Global Study of Online Violence against Women Journalists* (UNESCO & ICFJ, 2022), 1–325.

[٢٢] لمزيد من التفاصيل , ينظر:
Robert Chesney and Danielle Keats Citron, “Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security,” *California Law Review* Vol. 107:1753 (2019), https://doi.org/10.2139/ssrn.3213954.

[٢٣] ينظر:
Victoria Rousay, “Sexual Deepfakes and Image-Based Sexual Abuse: Victim-Survivor Experiences and Embodied Harms” (Master’s thesis, Harvard University, 2023), https://nrs.harvard.edu/URN-3:HUL.INSTREPOS:37374909.

[٢٤] ينظر : Ibid .

[٢٥] ينظر : احمد محمد فتحي الخولي, المسؤولية المدنية الناتجة عن الاستخدام غير المشروع لتطبيقات الذكاء الاصطناعي - الديب فيك نموذجا, مجلة البحوث الفقهية والقانونية , العد السادس والثلاثون, اكتوبر ٢٠٢١, ص ٢٦٠

[٢٦] ينظر :
Altij., “DEEP FAKES PORNOGRAPHIQUES : Que Dit La Loi ?,” ALTIJ Avocats, accessed April 19, 2025, https://www.altij.fr/en/news-details/deep-fake-et-revenge-porn-que-dit-la-loi.

[٢٧] ينظر : المادة ٢٢٦-٨ من قانون العقوبات الفرنسي رقم ٩٢-٦٨٣ المؤرخ ٢٢ يوليو ١٩٩٢ والنافذ لعام ١٩٩٤ وفق اخر تحديث بعد تعديل ٢٠٢٤.

[٢٨] ينظر : مرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ في شأن مكافحة الشائعات والجرائم الإلكترونية في الامارات

[٢٩] ينظر : المادة ٤٣٣ من قانون العقوبات العراقي رقم ١١١ لسنة ١٩٦٩ المعدل.

[٣٠] ينظر : عماد الدين حامد الشافعي، "المسؤولية الجنائية عن جرائم الذكاء الاصطناعي – دراسة مقارنة"، مجلة الحقوق للبحوث القانونية والاقتصادية , كلية الحقوق– جامعة الإسكندرية، المجلد ٢,٢٠١٩، العدد ٣، يوليو ٢٠١٩، الصفحة ٦٦٦-٤٧٩

[٣١] ينظر:
Julie Groffe-Charrier, “Vers un encadrement légal des deepfakes - IP/IT et Communication,” Dalloz Actualité, juillet 2023, https://www.dalloz-actualite.fr/flash/vers-un-encadrement-legal-des-deepfakes.

[٣٢] ينظر : المادة ٢٢٦-٨ من قانون العقوبات الفرنسي رقم ٩٢-٦٨٣ المؤرخ ٢٢ يوليو ١٩٩٢ والنافذ لعام ١٩٩٤ وفق اخر تحديث بعد تعديل ٢٠٢٤.

[٣٣] ينظر:
Christelle Coslin, Christine Gateau, and Alexis de Kouchkovsky., “France Prohibits Non-Consensual Deep Fakes,” www.hoganlovells.com, July 15, 2024, https://www.hoganlovells.com/en/publications/france-prohibits-non-consensual-deep-fakes.

[٣٤] ينظر : هيئة تنظيم الاتصالات والحكومة الرقمية ,"هيئة تنظيم الاتصالات والمجلس الإعلامي يطلقان حملة توعوية مشتركة حول سلامة العائلة على الإنترنت." , هيئة تنظيم الاتصالات والحكومة الرقمية، ١٨ أكتوبر ٢٠٢٣. تم الدخول إليه في ١ مايو ٢٠٢٥.
https://tdra.gov.ae/ar/media/press-release/2023/tdra-and-the-uae-media-council-launch-a-joint-campaign

[٣٥] لمزيد من التفاصيل , ينظر: معاذ سليمان الملا , " فكرة الحق في الدخول في طي النسيان الرقمي في التشريعات الجزائية الالكترونية الحديثة -دراسة مقارنة بين التشريع العقابي الفرنسي والتشريع الجزائي الكويتي" العدد (٣) - الجزء الأول - مايو ٢٠١٨ : ١١٧- ١٥٢

[٣٦] ينظر المادة ١٣١-٢١ من قانون العقوبات الفرنسي رقم ٩٢-٦٨٣ المؤرخ ٢٢ يوليو ١٩٩٢ والنافذ لعام ١٩٩٤.

[٣٧] لمزيد من التفاصيل , ينظر: منتدى المركز الدولي للصحفيين (IJNet). "استخدام الذكاء الاصطناعي في الكشف عن التزييف العميق في التحقيقات الاستقصائية." ، ٥ مارس ٢٠٢٥. تم الدخول إليه في ١ مايو ٢٠٢٥.
https://ijnet.org/ar/story/استخدام-الذكاء-الاصطناعي-في-الكشف-عن-التزييف-العميق-في-التحقيقات-الاستقصائية

[٣٨] ينظر :
Fakhar Abbas and Araz Taeihagh, “Unmasking Deepfakes: A Systematic Review of Deepfake Detection and Generation Techniques Using Artificial Intelligence,” *Expert Systems with Applications* 252 (October 15, 2024): 124260, https://doi.org/10.1016/j.eswa.2024.124260.

[٣٩] لمزيد من التفاصيل , ينظر: عمار باسر محمد البابلي," دور انظمة الذكاء الاصطناعي في التنبؤ بالجريمة", مجلة الامن والقانون, اكاديمة شرطة دبي, العدد (١) المجلد (٢٩), ٢٠٢١: ١٢٤- ٢١٣.

[٤٠] ينظر: شنتير خضرة, الاليات القانونية لمكافحة الجريمة الالكترونية- دراسة مقارنة , اطروحة دكتوراه مقدمة الى كلية الحقوق والعلوم السياسية, جامعة ادرار , الجزائر, ٢٠٢١, ص ١١٦ .

[٤١] ينظر : المصدر السابق ص ٢١٤

[٤٢] ينظر:

Gabriel Pestana, Luís M. Carvalho, and Sebastian Chmel, “The Data Governance Process Within the Digital Chain of Custody,” in *Paradigms on Technology Development for Security Practitioners*, ed. Ilias Gkotsis et al. (Cham: Springer Nature Switzerland, 2025), 3–14, https://doi.org/10.1007/978-3-031-62083-6_1.

[٤٣] ينظر: علاء الدين منصور مغايرة, "جرائم الذكاء الاصطناعي وسبل مواجهتها: جرائم التزييف العميق نموذجا", المجلة الدولية للقانون جـامعة قطـــر, ، المجلد الثالث عشر، العدد المنتظم الثاني، ٢٠٢٤, ص ١٤٢.

[٤٤] ينظر:

European Parliament News, “Digital Services Act: Agreement for a Transparent and Safe Online Environment,” April 23, 2022, https://www.europarl.europa.eu/news/en/press-room/20220412IPR27111/digital-services-act-agreement-for-a-transparent-and-safe-online-environment.

[٤٥] وفقًا للمادة ٤٢٠ من مرسوم بقانون اتحادي بشأن الإجراءات الجزائية لعام ٢٠٢٢، تسجل وتحفظ الإجراءات عن بُعد إلكترونيًا، ويجب أن تكون لها صفة السرية. ولا يجوز تداولها أو الاطلاع عليها أو نسخها من النظام المعلوماتي الإلكتروني إلا بإذن من النيابة العامة أو المحكمة المختصة حسب الأحوال

[٤٦] ينظر:

Council of Europe, “International Network of National Judicial Trainers [INJT],” Cybercrime, accessed May 1, 2025, https://www.coe.int/en/web/cybercrime/international-network-judicial-trainers-cybercrime.

[٤٧] ينظر: معهد دبي القضائي. "معهد دبي القضائي ينظم أول برنامج تدريبي لأعضاء النيابة العامة." مسبار للأخبار. تم النشر في ٢٠ فبراير ٢٠٢٥. تم الاطلاع عليه في ١ مايو ٢٠٢٥. https://mesbar.ae/uae/122034/

[٤٨] ينظر:

CNIL, “Informing Data Subjects,” CNIL, July 2, 2024, https://www.cnil.fr/en/informing-data-subjects.

[٤٩] ينظر: الإمارات اليوم. "الإمارات تحذر من تصديق محتوى التزييف العميق." ١٢ سبتمبر ٢٠٢٤ تاريخ الدخول ١ مايو ٢٠٢٥ https://www.emaratalyoum.com/local-section/other/2024-09-12-1.1881882 .

[٥٠] ينظر:

INTERPOL, “Beyond Illusions: Unveiling the Threat of Synthetic Media for Law Enforcement.,” Report, 2024., Report 2024.

[٥١] ينظر:

INTERPOL, “USD 300 Million Seized and 3,500 Suspects Arrested in International Financial Crime Operation,” INTERPOL, December 19, 2023, https://www.interpol.int/News-and-Events/News/2023/USD-300-million-seized-and-3-500-suspects-arrested-in-international-financial-crime-operation.

[٥٢] ينظر:

Council of Europe, “About the Convention - Cybercrime,” Cybercrime, accessed May 2, 2025, https://www.coe.int/en/web/cybercrime/the-budapest-convention.