

المكافحة الجنائية لظاهرة التزييف العميق باستخدام أنظمة الذكاء الاصطناعي في ضوء السياسة التشريعية المعاصرة (دراسة مقارنة تحليلية)

الأستاذ الدكتور / ياسر محمد المعني

أستاذ القانون الجنائي - كلية الشرطة - أكاديمية الشرطة - دولة قطر

Yasser-ellamey@hotmail.com

ملخص البحث

مما لا شك فيه أن التطور التكنولوجي في أنظمة وتقنيات الذكاء الاصطناعي كان له بالغ الأثر على تطور مستوى جودة المحتوى المرئي والصوتي في البيئة الرقمية ووسائلها المتنوعة، ولكن في نفس الوقت أدى هذه التطور في أنظمة الذكاء الاصطناعي إلى مساوئ تتمثل في انتشار ظاهرة التزييف العميق باستخدام أنظمة الذكاء الاصطناعي؛ مما يشكل معه خطورة على حقوق الإنسان، ومنها الحق في حريات الحصول على المعلومات دون أي تزييف أو تضليل أو خداع.

الأمر الذي يثير معه إشكالية حول ما مدى نجاعة الآليات والقواعد القانونية الحالية في مواجهة هذه الظاهرة الإجرامية، أما نحن ففي حاجة إلى قواعد قانونية خاصة تناسب هذه الظاهرة الإجرامية الجديدة، وذلك من خلال توضيح ماهية التزييف العميق باستخدام تقنيات الذكاء الاصطناعي، من خلال تحديد مفهوم التزييف العميق وخصائصه وتميزه عن غيره من جرائم التزييف التقليدية، كذلك عرض صور التزييف العميق باستخدام أنظمة الذكاء الاصطناعي، ثم نستعرض بعد ذلك الآليات القانونية للمكافحة الجنائية لظاهرة التزييف

العميق باستخدام أنظمة الذكاء الاصطناعي في ضوء مخاطر التزييف العميق الخطيرة على أمن المجتمع واستقراره، وما إذا كنا في حاجة إلى وجود قواعد قانونية خاص لتنظيم مكافحة الجنائية لهذه الظاهرة الإجرامية الحديثة، وفي النهاية نحاول الإجابة على تساؤل حول ما مدى إمكانية الاعتماد على الأدلة المستمدة من أنظمة الذكاء الاصطناعي في مجال الإثبات لتحقيق العدالة الجنائية.

الكلمات المفتاحية:

التزييف العميق - أنظمة الذكاء الاصطناعي - التزوير والتزييف - تزييف المحتوى الصوتي - تزييف المحتوى المرئي - الأدلة الجنائية الرقمية - الأدلة الجنائية الذكية.

Criminal Combating Deepfake Phenomenon Using Artificial Intelligence Systems

Yasser Mohamed Ellamey

Professor of Criminal Law

Police College, Police Academy, State of Qatar

Yasser-ellamey@hotmail.com

Abstract:

There is no doubt that the technological development in artificial intelligence systems and techniques has had a significant impact on the development of visual and audio content in the digital environment and its various media, including digital media, but at the same time this development in artificial intelligence systems has led to the spread of the phenomenon of deep forgery using artificial intelligence techniques. This poses a threat to human rights, including the right to freedom of access to information without any forgery, misleading or deception. This required studying it to clarify the nature of deep forgery using artificial intelligence techniques, by defining the concept of deep forgery, its characteristics and distinguishing it from other traditional forgery crimes, as well as displaying images of deep forgery using artificial intelligence techniques, then we review the legal mechanisms for criminally combating the phenomenon of deep forgery using artificial intelligence systems in light of the serious risks of deep forgery to the security and stability of society, in order to reach the extent of the importance of having a special law to criminally combat this modern criminal phenomenon, as well

as the extent to which it is possible to rely on smart and digital evidence in the field of proof to achieve criminal justice.

Keyword List:

Deepfake – Artificial Intelligence Systems – Forgery and Forgery – Audio Content
Forgery – Visual Content Forgery – Digital Forensics – Smart Forensics

المقدمة

إن التطور التكنولوجي في أنظمة وتقنيات الذكاء الاصطناعي والتعلم الآلي كان له بالغ الأثر على تطور المحتوى المرئي والصوتي في البيئة الرقمية ووسائطها المتنوعة ومنها وسائل الإعلام الرقمي، وأصبح لهذا المحتوى الرقمي القدرة على الانتشار والانتقال بطريقة سريعة وعلى نطاق واسع؛ مما يشكل معه مجالا خصبا من قبل الجناة لنشر الشائعات والأخبار الكاذبة والمحتوى الرقمي المزيف تزييفا عميقا وبدرجة عالية الدقة؛ للتأثير على الرأي العام وتغيير المواقف والاتجاهات حول الموضوعات التي تهم الرأي العام وتؤثر في المناخ الديمقراطي، كذلك استغلالها في مجال حروب الجيل الخامس من المعلومات والبيانات المضللة تجاه دولة ما.

ويرجع ظهور ظاهرة التزييف العميق (deep fake) إلى عام 2017، وذلك عندما قام أحد مستخدمي موقع التواصل الاجتماعي (Reddit) بنشر مقاطع فيديو معدلة لعدد من المشاهير من خلال استخدام خوارزميات أنظمة الذكاء الاصطناعي في تغيير وجه الشخص المتحدث الأصلي⁽¹⁾، واستبداله بشخص آخر على أنه المتحدث الحقيقي بطريقة محترفة يصعب معها على الشخص العادي التفرقة بين الفيديو المزيف والحقيقي. ثم أعقب ذلك تزايد إصدار العديد من التطبيقات التي تعمل على التزييف العميق للوجه باستخدام خوارزميات الذكاء الاصطناعي مثل: (Deep fake lab – Jiggy – Face swap live – Reface – Zao)⁽²⁾، وهذه التطبيقات جميعها تعتمد على تقنية التعرف الآلي على وجه الأشخاص عن طريق البيانات البيومترية للأفراد، وذلك استنادا إلى المعلومات والسمات السلوكية والبيولوجية المخزنة وذلك باستخدام خوارزميات أنظمة الذكاء الاصطناعي، وبالتالي أصبحت تشكل خطورة على حق الإنسان في حرية الحصول

1 - C. Neu Berghoff & A. Von Twickel, The interplay of AI and biometrics: challenges and opportunities, Computer, 54 (09), 2021, PP. 80 – 85.

2 - P. Li Q. Dong & J. Zheng, Enhancing the security of pattern unlock with surface EMG – based biometrics, Applied Sciences, 10 (2), 2020, p. 541.

على المعلومات دون أي تزيف أو تضليل أو خداع⁽¹⁾، وكذلك تمثل تهديدا خطيرا للأمن المعلوماتي السببراني عن طريق نشر الشائعات عبر الإنترنت والتطبيقات والبرامج عبر الهواتف الذكية من خلال المعلومات والبيانات المضللة والمزيفة عن طريق استخدام تقنيات التزييف العميق؛ مما يهدد أمن واستقرار الدولة ويهدد سلامة المجتمعات.

1 - أهمية الدراسة:

مما لا شك فيه أن مقاطع الفيديو – على اليوتيوب، والتيك توك، ومواقع التواصل الاجتماعي عبر الإنترنت، والتطبيقات الإلكترونية على الهواتف الذكية – أصبحت اليوم من أهم الأدوات الجاذبة والمؤثرة في سلوكيات جمهور المشاهدين لها على منصات التواصل الاجتماعية عبر الإنترنت والتطبيقات الإلكترونية المختلفة، وكذلك تناقلها وتداولها بشكل كثيف وكبير فيما بين الأشخاص، إلا أنه في الوقت نفسه ظهرت سلوكيات غير مشروعة تتمثل في التزييف العميق لهذه الفيديوهات ومقاطع الصوت ونشرها على المواقع الإلكترونية المختلفة، وبالتالي ساهم ذلك في انتشار ظاهرة التزييف العميق عبر الفيديوهات المزيفة باستخدام أنظمة الذكاء الاصطناعي، مثل: النظم الذكية الخبيرة والشبكات العصبية الذكية والشبكات التوليدية التنافسية ونظم الخوارزميات الذكية؛ مما يشكل معه ظاهرة إجرامية خطيرة تؤدي إلى تفشي المعلومات والأخبار الكاذبة والشائعات في المجتمع، والتي يكون لها تأثير وخيم على تضليل جمهور المشاهدين لها. مما يوجب على الباحثين تناول ما تثيره هذه الظاهرة الإجرامية من إشكاليات قانونية، وكذلك ضرورة تدخل المشرع بالنص على القواعد القانونية الكافية لمواجهة هذه الظاهرة الإجرامية الخطيرة التي تهدد أمن وسلامة استقرار المجتمع داخل الدول، من خلال اتباع سياسة تشريعية حديثة تتلاءم مع تطورات العصر الحالي، وفي الوقت نفسه تلاحق التقدم التكنولوجي وتقنيات أنظمة الذكاء الاصطناعي المستخدمة في ارتكاب هذا النوع من الجرائم.

1 - J. Wojewidka, The deepfake threat to face biometrics, Biometric Technology today, (2), 2020, pp. 5-7.

2 - إشكالية الدراسة:

ترتكز إشكالية الدراسة حول الإجابة عن تساؤل أساسي وهو، ما مدى كفاءة القواعد القانونية التقليدية في القانون الجنائي في مواجهة ظاهرة التزييف العميق باستخدام أنظمة الذكاء الاصطناعي؟ أما نحن ففي حاجة إلى وجود قواعد خاصة لمكافحة هذه الظاهرة الإجرامية المستحدثة؟ وللإجابة عن هذه الإشكالية سوف نستعرض في هذه الدراسة في البداية توضيح ماهية التزييف العميق باستخدام تقنيات الذكاء الاصطناعي من خلال تحديد مفهوم التزييف العميق وخصائصه وتميزه عن غيره من جرائم التزييف التقليدية، ثم نستعرض الآليات القانونية للمكافحة الجنائية لظاهرة التزييف العميق باستخدام أنظمة الذكاء الاصطناعي في ضوء مخاطر التزييف العميق الخطيرة على أمن المجتمع واستقراره، وخاصة فيما يتعلق بجرائم التزوير والتشهير والتحريض على الكراهية والتمييز العنصري والتضليل الانتخابي عبر تشوية سمعة السياسيين، كل هذه الصورة الإجرامية تتم من خلال التزييف العميق باستخدام أنظمة الذكاء الاصطناعي، خاصة في ظل غياب التشريعات الخاصة لمكافحة ظاهرة التزييف العميق باستخدام الذكاء الاصطناعي في العديد من التشريعات المقارنة.

كذلك نستعرض موقف السياسة التشريعية المقارنة في مواجهة هذه الظاهرة الإجرامية وخاصة موقف المشرع الأوروبي، وذلك في ظل اللائحة الأوروبية للخدمات الرقمية (DSA) والتي دخلت حيز النفاذ في 25 أغسطس 2023؛ حيث تناول المشرع الأوروبي فيها ظاهرة التزييف العميق عبر قسمين وهما على النحو التالي: (عندما تدرك منصة على الإنترنت أن جزءا من المحتوى عبارة عن صورة أو مقطع صوتي أو فيديو تم إنشاؤه أو التلاعب به، ويشبه الأشخاص أو الأشياء أو الأماكن أو الكيانات أو الأحداث الأخرى الحقيقية ويبدو أنه حقيقي؛ فيجب على المنصة أن تعلم المستخدمين أن هذا المحتوى غير أصلي).

وكذلك تناول المشرع الأوروبي للتدابير الوقائية لمواجهة هذه الظاهرة الإجرامية من

قبل شركات المنصات عبر الإنترنت، وقد قسم المشرع الأوروبي التزامات هذه الشركات إلى قسمين التزامات الشركات الكبيرة التي تحتوي على أكثر من 45 مليون مشترك، والتزامات الشركات الصغيرة في الالتزام بالتدابير. بالإضافة إلى ذلك فقد أصدر المشرع الأوروبي في 13 يونيو 2024 اللائحة الأوروبية بشأن الذكاء الاصطناعي رقم 1689 لسنة 2024، نص فيها على القواعد المتعلقة بتنظيم الذكاء الاصطناعي في ضوء إنشاء إطار قانوني موحد⁽¹⁾؛ بحيث تركز على ضمان مستوى عال من حماية وسلامة المجتمع وضمن الحقوق الأساسية للإنسان والمنصوص عليها في ميثاق الحقوق الأساسية للاتحاد الأوروبي، بما في ذلك ضمان مبادئ الديمقراطية وسيادة القانون.

وتأسيساً على ذلك؛ فسوف نحاول في هذه الدراسة الإجابة على التساؤلات التالية:

- 1- ماهية التزييف العميق باستخدام تقنيات الذكاء الاصطناعي.
- 2 - التفرقة ما بين التزييف العميق باستخدام تقنيات الذكاء الاصطناعي والتزييف التقليدي.
- 3 - أركان جريمة التزييف العميق باستخدام تقنيات الذكاء الاصطناعي.
- 4 - آليات المواجهة الجنائية لظاهرة التزييف العميق باستخدام الذكاء الاصطناعي.

3 - منهجية الدراسة:

تعتمد دراسة موضوع مكافحة الجنائية لظاهرة التزييف العميق باستخدام أنظمة الذكاء الاصطناعي على المنهج العلمي الوصفي من أجل تحديد ماهية التزييف العميق باستخدام أنظمة الذكاء الاصطناعي؛ بحيث نستعرض مفهوم التزييف العميق وخصائصه وصوره، كذلك استخدام المنهج العلمي المقارنة في هذه الدراسة؛ بحيث نقارن ما بين موقف المشرع في الدولة العربية، مثل: المشرع القطري، والمشرع المصري، والمشرع الإماراتي، مع موقف

1 - انظر: اللائحة الأوروبية الجديدة بشأن الذكاء الاصطناعي رقم 1689 لسنة 2024، والصادرة في 13 يونيو 2024، وقد دخلت بعض قواعدها حيز النفاذ في الثاني من أغسطس 2024، وباقي القواعد سوف تدخل حيز النفاذ في العامين 2025 و2026.

المشرع في الدول الغربية، مثل: المشرع الفرنسي، والمشرع الأمريكي، وكذلك موقف المشرع الأوروبي في مكافحة ظاهرة التزييف العميق باستخدام أنظمة الذكاء الاصطناعي؛ خاصة في ضوء اللائحة الأوروبية الجديدة بشأن الخدمات الرقمية واللائحة الأوروبية بشأن الذكاء الاصطناعي الصادرة في 13 يونيو 2024.

بالإضافة إلى ما سبق سوف نعتمد على المنهج العلمي التحليلي لتوضيح أركان جريمة التزييف العميق باستخدام أنظمة الذكاء الاصطناعي، وكذلك تحديد مع نجاعة آليات المواجهة الجنائية للتزييف العميق باستخدام الذكاء الاصطناعي؛ سواء من خلال التدابير الاحترازية والوقائية لمكافحة هذه الظاهرة الإجرامية أم من خلال التعاون الدولي فيما بين الدول لمكافحتها، كذلك مدى إمكانية الاعتماد على الأدلة الرقمية والذكية في الإثبات أمام المحاكم؛ لتحقيق العدالة الجنائية في ضوء احتمالية تزييفها بواسطة أنظمة الذكاء الاصطناعي.

4 - خطة الدراسة:

تنقسم خطة الدراسة إلى مطلبين، وذلك على النحو التالي:

المطلب الأول: ماهية التزييف العميق باستخدام تقنيات الذكاء الاصطناعي

الفرع الأول: مفهوم التزييف العميق باستخدام تقنيات الذكاء الاصطناعي في ضوء السياسة الجنائية المعاصرة

الفرع الثاني: صور التزييف العميق باستخدام تقنيات الذكاء الاصطناعي والتفرقة بينها وبين التزييف التقليدي

المطلب الثاني: أركان جريمة التزييف العميق باستخدام تقنيات الذكاء الاصطناعي

الفرع الأول: الركن المادي لجريمة التزييف العميق باستخدام الذكاء الاصطناعي

الفرع الثاني: الركن المعنوي لجريمة التزييف العميق باستخدام الذكاء الاصطناعي

الفرع الثالث: آليات المواجهة الجنائية للتزييف العميق باستخدام الذكاء الاصطناعي

المطلب الأول

ماهية التزييف العميق باستخدام تقنيات الذكاء الاصطناعي

في البداية وقبل أن نتناول موضوع المواجهة الجنائية لظاهرة التزييف العميق باستخدام تقنيات الذكاء الاصطناعي لا بد من توضيح أن هناك العديد من الاستخدامات المشروعة لتطبيقات التزييف العميق باستخدام تقنيات الذكاء الاصطناعي في مختلف المجالات والتي لا يعاقب عليها القانون، وذلك على النحو التالي⁽¹⁾:

- 1 - الاستخدامات المشروعة للتزييف العميق باستخدام تقنيات الذكاء الاصطناعي في مجال التطبيقات الطبية؛ حيث يتم في هذه الحالة استخدام التزييف العميق من أجل إنشاء صور طبية حديثة لأغراض التدريب العملي للطلاب في الحقل الطبي، مثل: صور الرنين المغناطيسي، وصور الأشعة، وغيرها من الصور الطبية الأخرى التي تستخدم في العملية التعليمية لطلاب المجال الصحي.
- 2 - الاستخدامات المشروعة للتزييف العميق باستخدام تقنيات الذكاء الاصطناعي في مجال الترفيه، مثال على ذلك: صناعة الأفلام والإعلانات من أجل تحسين جودة المحتوى الإعلاني، وصناعة الأفلام بواسطة إنشاء المؤثرات الصوتية والبصرية غير الحقيقية؛ لصنع مشاهد سينمائية متحركة أو التلاعب بالوجه بما يخدم صناعة السينما والترفيه وصناعة الإعلانات والدعاية التسويقية للسلع والخدمات.
- 3 - الاستخدامات المشروعة للتزييف العميق باستخدام تقنيات الذكاء الاصطناعي في المجال التعليمي؛ حيث يتم اصطناع مقاطع الفيديو والصور ومقاطع الصوت التي تخدم العملية التعليمية وتساعد الطلاب على فهم المحتوى التعليمي الصعب؛ خاصة في مجالات العلوم المعقدة والمتقدمة التي تحتاج من الطلاب بذل الجهد الكبير من أجل اكتساب المهارات والمعارف التعليمية والمهنية في مجال تخصصهم.

1 - دليل التزييف العميق، البرنامج الوطني للذكاء الاصطناعي، دولة الإمارات العربية المتحدة، يوليو 2021، ص 11.

4 - الاستخدامات المشروعة للتزييف العميق باستخدام تقنيات الذكاء الاصطناعي في خدمة العملاء، مثال على ذلك: المساعد الافتراضي، فمن أجل تحسين جودة ومستوى تقديم الخدمة للعملاء يتم الاستعانة بالمساعد الافتراضي بالصوت والصورة في مراكز الاتصال من أجل تقديم الخدمة للعملاء بجودة ومستوى عالي الدقة والمهارة، مثال على ذلك: الخدمات التفاعلية البنكية بالصوت والصورة عبر أجهزة الصرافة البنكية، والتي يستطيع من خلالها العميل التحدث بالصوت والصورة مع الأشخاص الافتراضية وطلب الخدمة البنكية.

أما بالنسبة لمواجهة للاستخدامات غير المشروعة لتقنيات الذكاء الاصطناعي للتزييف العميق في مجال الخدمات الرقمية؛ فقد نص المشرع الأوروبي في اللائحة الأوروبية للخدمات الرقمية (DSA) والصادرة في يوليو 2022 والتي دخلت حيز النفاذ في 25 أغسطس 2023 على أنه في حالة التزييف العميق المشروع باستخدام تقنيات الذكاء الاصطناعي لا بد وأن تقوم المنصات الكبيرة عبر الإنترنت⁽¹⁾ بتحديد أن المحتوى الصوتي أو مقطع الفيديو أو الصورة مزيفة بشكل واضح وصريح لمتلقي الخدمات الرقمية⁽²⁾. وبناء على ذلك يتم منح الإذن بالممارسة المشروعة للتزييف العميق للشركات التي تحتاج إلى القيام بهذه الممارسات، وتطبيقاً لذلك؛ فقد تم منح الإذن بمبادلة الوجه في المواد الترويجية والدعاية الإعلانية لشركة (TelcoTelefon) الروسية بشأن الترخيص بهوية بروس ويليس في الحملة الإعلانية لخدماتها الرقمية⁽³⁾.

في هذا المطلب سوف نستعرض في البداية مفهوم التزييف العميق وخصائصه في الفرع الأول، وفي الفرع الثاني سوف نتناول بالتحديد أوجه الفرق ما بين التزييف العميق باستخدام تقنيات الذكاء الاصطناعي والتزييف التقليدي.

1 - يقصد بالمنصات عبر الإنترنت الكبيرة بأنها: هي المنصات التي يزيد عدد المتابعين لها عن عدد 45 مليون مشترك.

2 - انظر: المادة 63 من اللائحة الأوروبية للخدمات الرقمية (DSA) والصادرة في يوليو 2022، ودخلت حيز النفاذ في سبتمبر 2023.

3 - أ. مارتن أندرسون، مقترحات تنظيم التزييف العميق لأوروبا والمملكة المتحدة، في 9 ديسمبر 2022، الموقع الإلكتروني: <https://www.unite.ai/ar/european-and-uk-deepfake-regulation-proposals-are-surprisingly-limited/>

تاريخ الزيارة 30 أغسطس 2024.

الفرع الأول

مفهوم التزييف العميق باستخدام تقنيات الذكاء الاصطناعي في ضوء السياسة الجنائية المعاصرة

سوف نحدد في البداية مفهوم التزييف العميق باستخدام تقنيات الذكاء الاصطناعي (أولاً)، ثم بعد ذلك نستعرض موقف السياسة الجنائية المعاصرة في مواجهة ظاهرة للتزييف العمق باستخدام تقنيات الذكاء الاصطناعي (ثانياً)، و(ثالثاً) نتناول – بالعرض – خصائص جرائم التزييف العميق باستخدام أنظمة الذكاء الاصطناعي.

أولاً: مفهوم التزييف العميق باستخدام تقنيات الذكاء الاصطناعي:

يقصد بالتزييف العميق بأنه استخدام تقنيات التوليف للوسائط المتعددة من خلال تقنيات الذكاء الاصطناعي، والتي يمكن من خلالها تركيب ملفات الصوت أو الفيديو للملف بطريقة تخالف الحقيقة، فعلى سبيل المثال: تغيير وجه الشخص على مقطع الفيديو أو استبدال صوت الشخص المتحدث بصوت آخر عن طريق إعادة إنتاج صوت الشخص بكلام لم يتحدث به⁽¹⁾. ويقصد بتقنية التزييف العميق بأنه تقنية تعتمد على المزج بين التعلم العميق والتزييف للحقيقة باستخدام تقنيات وخوارزميات الذكاء الاصطناعي، ومثال على ذلك: مقاطع الفيديو التي يتم تزييفها عن طريق التلاعب والاصطناع المفبرك؛ بحيث يتم تصوير أشخاص يقولون

1 -Tribunal correctionnel de Versailles - 8e ch. Correctionnelle, 8e ch., 14 avril 2021 / n° 20167000022, Sit:

[86](https://www.dalloz.fr/documentation/Document?id=TCORRVERSAILLES_2021-0414_20167000022&ctxt=0_YSR0MD1EZVWwRmFrZcKneCRzZj1zaW1wbGUtc2VhcmNo&ctxtl=0_cyRwYWdITnVtPTHCP3MkdHJpZGF0ZT1GYWxzZcKncyRzb3J0PSNkZWZhdWx0X0Rlc2PCp3Mkc2xOYIBhZz0yMMKncyRpc2Fibz1UcnVl wqdzJHBhZ2luZz1UcnVlwqdzJG9uZ2xldD3Cp3MkZnJlZXNjb3BIPUZhbHNIwqdzJHd vSM9RmFsc2XCp3Mkd29TUENIPUZhbHNIwqdzJGZsb3dNb2RIPUZhbHNIwqdzJGJxPcKncyRzZWFrY2hMYWJlY2VhcmNoQ2xhc3M9#texte-integral, V., Le 4 avril 2024.</p>
</div>
<div data-bbox=)

ويفعلون أشياء لم تحدث في الحقيقة⁽¹⁾، وفي هذه الحالة نجد أن تقنية التزييف العميق باستخدام تقنيات الذكاء الاصطناعي تعتمد بشكل أساسي على الشبكات العصبية للذكاء الاصطناعي التي تقوم بتحليل ومعالجة مجموعة من البيانات والمعلومات الرقمية بطريقة آلية، من أجل تقليد تعبيرات وجه الشخص المعني المراد تزييف صوته وصورته وتصرفاته⁽²⁾ من خلال إحدى تقنيات أنظمة الذكاء الاصطناعي؛ بحيث تبدو للشخص العادي واقعية وحقيقية على خلاف الواقع.

وعلى العكس مما سبق؛ فقد ذهب جانب من الفقه إلى تبني الاتجاه الموسع في تعريف التزييف العميق باستخدام تقنيات الذكاء الاصطناعي؛ بحيث يعرفه بأنه كل تلاعب في مقطع فيديو أو صوت من خلال خوارزميات الذكاء الاصطناعي من أجل جعله قابلاً للتصديق على أنه حقيقي للشخص العادي، وذلك سعياً من الجناة إلى استخدام التزييف العميق في نشر المعلومات والبيانات المضللة بطريقة أسرع عبر وسائل التواصل الاجتماعي الإلكترونية⁽³⁾ وبالتالي التأثير في جمهور المشاهدين والمتابعين؛ مما يؤثر على أمن واستقرار الدول، ومثال على ذلك: أن يقوم الشخص باصطناع أحداث غير حقيقية أو جعل أشخاص حقيقيين يقولون أشياء لم يقولوها أو لم يفعلوها من أجل تشوية سمعة الأشخاص السياسيين، أو تضليل جمهور الناخبين والتأثير على الحياة الديمقراطية ومبدأ سيادة القانون.

وانطلاقاً مما سبق؛ فقد نص المشرع الأوروبي في لائحة الخدمات الرقمية (DSA) والتي صدرت في يوليو 2022 ودخلت حيز النفاذ في 25 أغسطس 2023 على تعريف التزييف العميق

- 1 - S. G. Tesfagergish, R. Damasevicius & J. KAPOCIUTE - Dzikien, Deep fake recognition in tweets using text augmentation, Word embeddings and deep learning, In International conference on computational science and its applications, September, 2021, pp. 523 – 538.
- 2 - K. M. Saylor & L. A. Harris, Deep fakes and national security, Congressional research SVC Washington, USA, 2020.
- 3 - L. Laishram, M. M. Rahman & S. K. Jung, Challenges and applications of face deepfake, In international workshop on frontiers of computer vision, Springer, Cham, February, 2021, pp. 131- 156.

بأنه⁽¹⁾: "جزءاً من المحتوى عبارة عن صورة أو محتوى صوتي أو مقطع فيديو تم اصطناعه أو تم التلاعب به، دون موافقة الشخص المعني، ويشبه بشكل ملحوظ الأشخاص أو الأشياء أو الأماكن أو الكيانات أو الأحداث الأخرى الموجودة؛ بحيث يظهر بشكل خاطئ للشخص العادي على أنه حقيقي على خلاف الواقع". ويتضح من ذلك أن المشرع الأوروبي قد تبني الاتجاه التشريعي الحديث الذي ينظم من خلال القواعد القانونية الخاصة آليات مكافحة لظاهرة التزييف العميق للمحتوى الصوتي أو مقاطع الفيديو أو الصور من أجل توفير الحماية القانونية لمستخدمي المواقع الإلكترونية والتطبيقات ومواقع وسائل التواصل الاجتماعي عبر الإنترنت من أي تزييف للمحتوى يؤدي إلى إيقاع متلقي الخدمات الرقمية في الغلط أو اللبس أو يكون من شأنه أن يؤدي إلى ذلك.

وتأسيساً على ذلك؛ فقد أوجب المشرع الأوروبي على المنصات الكبيرة عبر الإنترنت ضرورة اتخاذ تدابير وقائية لمواجهة هذه الظاهرة الإجرامية والتي تتمثل في الالتزام بتحديد ما إذا كان المحتوى المعروض غير حقيقي ومزيف بطريقة واضحة لمتلقي الخدمات الرقمية، علاوة على ذلك القيام بمحو كل محتوى غير قانوني وهو ما سوف نتناوله بالتوضيح في المطلب الأخير.

ثانياً: موقف السياسة الجنائية المعاصرة من مواجهة ظاهرة التزييف العميق باستخدام أنظمة الذكاء الاصطناعي:

بادئ الأمر؛ كان الشكل المتعارف عليه من الجناة ارتكاب تزييف المحتوى الصوتي أو المرئي من خلال قيامهم باستخدام أدوات للتلاعب في الصورة والصوت بالأساليب التقليدية لتحريف المحتوى؛ مما كان يتطلب من الجناة – مرتكبي هذه الجرائم – التمتع بمهارات فنية عالية لتزييف هذا المحتوى؛ سواء كان مرئياً أم صوتياً، لكن مع ظهور تقنيات وحلول أنظمة الذكاء الاصطناعي أصبح متاحاً للأشخاص العاديين من الجناة إمكانية استخدام تقنيات

1 - انظر: المادة 30 من اللائحة الأوروبية الجديدة المتعلقة بالخدمات الرقمية (DSA) وقد دخلت حيز النفاذ في 25 أغسطس 2023.

الذكاء الاصطناعي في التزييف العميق عن طريق إنشاء محتوى مزيف للفيديوهات والصور والصوت من أجل انتحال شخصية أو الهوية الشخصية للغير وتقديم معلومات وبيانات مزيفة عن أنشطتهم وسلوكياتهم أو البيئة المحيطة بهؤلاء الأشخاص محل جريمة التزييف العميق باستخدام خوارزميات الذكاء الاصطناعي دون موافقتهم.

وقد شهد العالم في عام 2014 تحولا كبيرا في مجال تقنيات الذكاء الاصطناعي؛ بحيث أصبح في الإمكان إنشاء مقاطع فيديو وصوت مماثلة للمقاطع الأصلية عن طريق تطوير تقنيات التعلم الآلي العميق والمعقدة بواسطة الشبكات التوليدية التنافسية (Generative adversarial networks)، ونتيجة لذلك؛ فقد استغل الجناة هذه الميزة في ارتكاب جرائم التزييف العميق باستخدام تقنيات الذكاء الاصطناعي بواسطة إنتاج بيانات ومعلومات جديدة مزيفة لتهديد وابتزاز بعض الأفراد أو التشهير بسمعة السياسيين والأشخاص المشهورين، أو استخدام هذه الفيديوهات في تضليل أفراد المجتمع ونشر الشائعات والبيانات والمعلومات الكاذبة من أجل الإضرار بأمن وسلامة المجتمع عن طريق التلاعب بالرأي العام وتضليله؛ مما يؤثر على الحياة الديمقراطية، أو خلق أدلة مزيفة للتأثير على أحكام المحاكم القضائية⁽¹⁾، وبالتالي التشكيك في النزاهة والعدالة القانونية ومبدأ سيادة القانون.

وعقب ذلك؛ فقد تم التوسع في استخدام تقنيات الذكاء الاصطناعي في التزييف العميق، وذلك بشكل أساسي لإنشاء مقاطع فيديو إباحية مزيفة في عام 2017 من أجل الانتقام الإباحي أو الجنسي، وفي إنتاج فيديوهات مزيفة للسياسيين أو الفنانين من ذوي المكانة العالمية، وذلك من أجل تشويه سمعتهم السياسية أو الفنية أو من أجل ابتزازهم للحصول على المال

1 - مثال على ذلك استخدام تقنية استبدال الوجه (Face Swapping) عبر تقنيات الشبكات التوليدية التنافسية؛ حيث تعمل هذه التقنية على استبدال الوجه من خلال معالجة البيانات لوجه المستخدم، واستبدال وجه الشخص المراد تزييف بياناته عن طريق استخدام خوارزميات الذكاء الاصطناعي عبر التطبيقات الإلكترونية على الهواتف الذكية. وفي مثال آخر، استخدام تطبيقات الذكاء الاصطناعي على الهواتف الذكية في التلاعب في الصور أو الصوت عبر تقنية تحرير الصورة أو الصوت لأحد الأشخاص المدعوم بتقنية تعلم الآلة.

وذلك باستخدام تقنيات الذكاء الاصطناعي. وفي عام 2019 قامت شركة سامسونج باستخدام نظام يمكنه إنشاء مقاطع الفيديو غير حقيقية لشخص ما، من خلال استخدام صورة واحدة ثابتة وذلك عبر تقنية التعلم الآلي في التمكن من التعرف على تركيب وحركات وجه شخص ما⁽¹⁾، عقب ذلك يتم تركيب هذا القناع على وجه شخص آخر يتحدث في مقطع الفيديو من أجل اصطناع مقطع فيديو مزيف تزييفا عميقا باستخدام خوارزميات الذكاء الاصطناعي.

ولخطورة هذه الظاهرة الإجرامية؛ فقد تناول تقرير الاتحاد الأوروبي عن الاستخدامات والتجاوزات غير المشروعة للذكاء الاصطناعي بعض التوصيات، ومنها: ضرورة أن يقوم الاتحاد الأوروبي والدول الأعضاء بالنص على المواجهة الجنائية لظاهرة التزييف العميق باعتبارها من الظواهر الإجرامية الحديثة سريعة الانتشار في العصر الرقمي والذكاء الاصطناعي ومن أجل مواكبة المتغيرات التكنولوجية الحديثة، وذلك من خلال اتباع سياسة تشريعية معاصرة وفعالة لمكافحة الاستخدامات غير المشروعة لتقنية التزييف العميق باستخدام خوارزميات الذكاء الاصطناعي على المدى الطويل، دون أي إعاقة لإمكانيات الاستخدام المشروع لهذه التقنية التكنولوجية الحديثة.

وتطبيقا على ذلك؛ فقد أصدرت لجنة الرقمية والثقافية والإعلام في البرلمان البريطاني تقريرا عن مشروع قانون الأمان على الإنترنت في عام 2021، تدعو فيه الحكومة البريطانية إلى سرعة التنظيم القانوني لاستخدامات تقنية التزييف العميق بشكل استباقي⁽²⁾، مع التفرقة ما بين الاستخدامات المشروعة لهذه التقنيات والممارسات غير المشروعة التي قد تمثل نوعا من إساءة للتعامل مع الأطفال، أو نوعا من أنواع العنف عبر الإنترنت باعتبارها في النهاية تندرج 1 - أ. ماري شروتر، الذكاء الاصطناعي ومكافحة التطرف العنيف، تقرير في منشورات الشبكة العالمية لمكافحة التطرف التكنولوجي (GNET)، ص 17، على الموقع الإلكتروني: www.gent-research.org

تاريخ الزيارة 2 سبتمبر 2024.

2 - انظر: تقرير اللجنة الرقمية والثقافية والإعلام والرياضة، البرلمان البريطاني، مشروع قانون الأمان على الإنترنت، عام 2021.

تحت المحتوى الضار غير القانوني؛ حيث يقتصر التجريم القانوني في التشريع البريطاني على حالة التزييف العميق من أجل الانتقام الإباحي فقط، دون تناول الصور الأخرى لحالات التزييف العميق.

أما بالنسبة لموقف المشرع الأمريكي؛ فنجد أن هناك العديد من الولايات الأمريكية التي نص فيها قانون الولاية على تجريم التزييف العميق مثال ولاية تكساس؛ ففي عام 2019 أصدر مجلس الشيوخ في تكساس قانونا يحظر استخدام تقنية التزييف العميق في المجال السياسي، أما في ولاية فرجينيا؛ فقد تم تعديل القانون لينص على تجريم إنشاء صور أو مقاطع الفيديو غير حقيقية للغير عن طريق تقنية التزييف العميق، بالإضافة إلى النشر أو البيع غير المشروع لصور الغير. أما في ولاية كاليفورنيا ففي عام 2020؛ تم إدخال تعديلات على القانون بحيث أصبح ينص على حظر إنتاج أو نشر مقاطع الفيديو والصور المزيفة تزييفا عميقا باعتبارها إحدى صور جريمة التزييف العميق⁽¹⁾، ويتضح من ذلك أن المشرع الأمريكي في الولايات الأمريكية قد سعى مبكرا لمواجهة هذه الظاهرة الإجرامية لخطورتها على أمن واستقرار المجتمع الاجتماعي والسياسي.

أما بالنسبة لموقف المشرع المصري فباستقراء القوانين ذات الشأن نجد أن المشرع المصري قد نص على حماية حق الشخص في الصورة والصوت وعدم جواز انتحال هويته الشخصية، وذلك من خلال قانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018؛ حيث نص فيه المشرع المصري على تعريف البيانات والمعلومات الإلكترونية بأنه: "كل ما يمكن إنشاؤه أو تخزينه، أو معالجته أو تخليقه أو نقله، أو مشاركته، أو نسخه بواسطة تقنية المعلومات، مثال على ذلك الأرقام والأكواد والشفرات والحروف والرموز والإشارات والصور

1 - انظر: القانون رقم 751 (SB751)، ولاية تكساس، مجلس الشيوخ، عام 2019، وكذلك مشروع قانونية مجلس ولاية كاليفورنيا 602 (AB 602)، ولاية كاليفورنيا، 2020.

والأصوات، وما في حكمها"⁽¹⁾. وتأسيسا على ذلك نستطيع القول بأن المشرع المصري يعتبر الصور أو الأصوات التي يتم تزييفها من خلال خوارزميات الذكاء الاصطناعي محل حماية قانونية وفقا لقانون مكافحة جرائم تقنية المعلومات رقم 175 لسنة 2018، باعتبارها صورة من صور جرائم تقنية المعلومات في شكل التزييف العميق. علاوة على ذلك؛ فقد نص المشرع المصري على حماية الحق في البيانات الشخصية من كافة صور الانتهاك، وذلك من خلال القانون رقم 151 لسنة 2020 والذي نص فيه على حماية البيانات الشخصية؛ أي البيانات المتعلقة بالشخص الطبيعي المحدد، أو الذي يمكن تحديده؛ سواء كان ذلك بشكل مباشر أم غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخرى كالاسم، أو الصوت أو الصورة، أو رقم تعريفى أو محدد للهوية عبر الإنترنت، أو أي بيانات تحدد الهوية النفسية، أو الصحية أو الاقتصادية، أو الثقافية أو الاجتماعية⁽²⁾. ويتضح من تعريف المشرع المصري للبيانات الشخصية محل الحماية أن المشرع يحمي حق الشخص في الصورة والصوت – باعتبارهما من البيانات الشخصية – من استغلالهما في ارتكاب الجرائم، ومنها جريمة التزييف العميق باستخدام خوارزميات الذكاء الاصطناعي محل الدراسة، ولكن حتى الآن لا يوجد نص قانوني واضح ومباشر لمواجهة التزييف العميق باستخدام أنظمة وتقنيات الذكاء الاصطناعي.

أما بالنسبة لموقف المشرع القطري؛ فنجد أنه لم ينص صراحة على تجريم ظاهرة التزييف العميق باستخدام تقنيات وأنظمة الذكاء الاصطناعي، ولكن في نفس الوقت توسع في تعريف الجريمة الإلكترونية؛ فقد نص في قانون مكافحة الجرائم الإلكترونية على تعريفها بأنها: "كل فعل ينطوي على استخدام وسيلة تقنية المعلومات أو نظام معلوماتي أو الشبكة المعلوماتية،

1 - انظر: الفقرة الثالثة من المادة الأولى من التعريفات من القانون المصري رقم 175 لسنة 2018 بشأن مكافحة جرائم تقنية المعلومات، والمنشور في الجريدة الرسمية، العدد رقم 32 مكرر (ج)، والصادر في 14 أغسطس 2018، ص 3.
2 - انظر: المادة الأولى التعريفات من القانون المصري رقم 151 لسنة 2020 بشأن حماية البيانات الشخصية، والمنشور في الجريدة الرسمية، العدد رقم 28 مكرر (هـ) والصادرة في 15 يولييه 2020، ص 4.

بطريقة غير مشروعة، بما يخالف القانون⁽¹⁾. علاوة على ذلك؛ فقد نص المشرع القطري في نفس القانون على تجريم كل تعدي على المبادئ أو القيم الاجتماعية، أو نشر أخبار أو صور أو تسجيلات صوتية أو مرئية تتصل بحرمة الحياة الخاصة أو العائلية للأشخاص، ولو كانت صحيحة، أو تعدي على الغير بالسب أو القذف، عن طريق استخدام الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات⁽²⁾. وبالتالي يجب أن يستظهر الحكم توفر محل هذه الجرائم وهي مقاطع الفيديو أو الصور التي يتم نشرها على الشبكة المعلوماتية أو وسائل تقنية المعلومات ويخضع ذلك لرقابة محكمة التمييز.

وتطبيقاً لذلك فقد قضت محكمة التمييز القطرية بأنه: "لكي يتحقق النموذج الإجرامي - لهذا الوصف - أن يستظهر الحكم في مدوناته تلك المقاطع - التي هي جوهر الواقعة المسندة للطاعن؛ طبقاً لوصف النيابة العامة - حتى تستطيع هذه المحكمة - محكمة التمييز - من مراقبة صحة التطبيق القانوني على الواقعة كما أوردها الحكم، وكان من المقرر أنه يتعين على الحكم الصادر بالإدانة أن يورد واقعة الدعوى على نحو تتحقق به أركان الجريمة التي دان الطاعن بها، وأن يورد مؤدى الأدلة على نحو كاف، وهو ما خلا منه الحكم المطعون فيه؛ بما يوجب تمييزه، والإعادة"⁽³⁾.

وعلى ضوء ذلك؛ يتضح لنا أن المشرع القطري قد تبنى الاتجاه الموسع في مكافحة الجرائم الإلكترونية؛ فلم يتطلب في هذه النوع من الجرائم تقديم شكوى من أجل تحريك

1 - انظر: المادة الأولى تعريفات من قانون مكافحة الجرائم الإلكترونية القطري، رقم 14 لسنة 2014، والمنشور في الجريدة الرسمية العدد 15، والصادرة بتاريخ 2 أكتوبر 2014.

2 - حيث تنص المادة الثامنة من قانون مكافحة الجرائم الإلكترونية على أنه: «يعاقب بالحبس مدة لا تتجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (100,000) مائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من تعدى على أي من المبادئ أو القيم الاجتماعية، أو نشر أخباراً أو صوراً أو تسجيلات صوتية أو مرئية تتصل بحرمة الحياة الخاصة أو العائلية للأشخاص، ولو كانت صحيحة، أو تعدى على الغير بالسب أو القذف، عن طريق الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات».

3 - محكمة التمييز القطرية، تمييز جنائي، جلسة 21 ديسمبر 2020، الطعن رقم 163 لسنة 2020.

الدعوى الجنائية على خلاف جرائم السب والقذف التقليدية، وتطبيقا لذلك فقد قضت محكمة التمييز القطرية بأن: "المادة الثالثة من قانون الإجراءات الجنائية القطري قد جرى نصها بأنه: "لا يجوز تحريك الدعوى الجنائية إلا بناء على شكوى من المجني عليه، أو من يقوم مقامه في الجرائم المنصوص عليها في المواد أرقام: (....) من قانون العقوبات القطري، وكذلك في الجرائم الأخرى التي ينص عليها القانون"، كما أن المادة (10) منه نصت أيضا على أن لمن قدم الشكوى أن يتنازل عنها في أي وقت إلى أن يصدر حكم بات في الدعوى، ورتب على ذلك انقضاء الدعوى الجنائية بالتنازل. وكان البين من الأوراق أن الجريمتين اللتين قدم بهما الطاعن من النيابة العامة وتم إدانته عنهما معاقب عليهما بالمادتين (9,8) من القانون رقم (14) لسنة 2014 بإصدار قانون مكافحة الجرائم الإلكترونية القطري، وقد خلا القانون المذكور صراحة من تقييد حرية النيابة العامة في تحريك الدعوى عنهما وسائر ما ورد به من جرائم على تقديم شكوى من المجني عليه، كما فعل ببعض الجرائم المنصوص عليها بالمادة (3) من قانون الإجراءات الجنائية سالفه الذكر، والتي لم يقدم الطاعن لمعاقبته وفقا لأي منها، ومن ثم فإن ما يثيره الطاعن في هذا الشأن، بصدد تحريك الدعوى أو انقضائها بالتنازل يكون غير مقبول، ولا على المحكمة إن لم تعرض لدفاعه في هذا الشأن وإن كان الحكم المطعون فيه عرض إليه واطرحه بما يتفق مع هذا النظر السابق"⁽¹⁾.

بالإضافة إلى ذلك؛ فقد جرم المشرع القطري كل استخدام للشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات في تهديد أو ابتزاز شخص لحمله للقيام بعمل أو الامتناع عنه⁽²⁾. ومنها بالتأكيد استخدام مقاطع الفيديو والصور المزيفة تزييفا عميقا باستخدام تقنيات الذكاء

1 - محكمة التمييز القطرية، تمييز جنائي، جلسة 3 فبراير 2020، الطعن رقم 139 لسنة 2020.

2 - حيث تنص المادة التاسعة من قانون مكافحة الجرائم الإلكترونية رقم 14 لسنة 2014 على أنه: «يعاقب بالحبس مدة لا تجاوز ثلاث سنوات، وبالغرامة التي لا تزيد على (100,000) مائة ألف ريال، أو بإحدى هاتين العقوبتين، كل من استخدم الشبكة المعلوماتية أو إحدى وسائل تقنية المعلومات، في تهديد أو ابتزاز شخص، لحمله على القيام بعمل أو الامتناع عنه».

الاصطناعي في التهديد أو الابتزاز الإلكتروني لحمل شخص على القيام بعمل أو الامتناع عنه على غير إرادته.

وتطبيقاً لذلك؛ فقد قضت محكمة التمييز القطرية بأنه: "جريمة التهديد وفقاً للنص سالف البيان تتطلب أن يستخدم الجاني الشبكة المعلوماتية التي تتمثل في الشبكات الخاصة والعامة أو الشبكة العالمية "الإنترنت" وأن يكون التهديد بغرض حمل شخص على القيام بعمل أو الامتناع عنه على غير إرادته ويجب أن يتوفر الغرض وقت ارتكاب فعل التهديد، ولم يشترط المشرع أن يكون التهديد علانية أمام جمع فيكفي أن يكون في شبكة خاصة بل تقع الجريمة بمجرد استخدام الجاني الإنترنت في ارتكابها - كما هو الحال في الدعوى الحالية - مؤدى ذلك أن استخدام الجاني برنامج "الواتساب" الذي يعمل بالإنترنت في إرسال رسائل التهديد للمجني عليه لإرغامه على التنازل عن دعوى التزوير - المتداولة في ذلك الوقت - تتحقق به جريمة التهديد كما هي معرفة بالمادة سالفة البيان، ولا يغير من ذلك القضاء بالبراءة في قضية التزوير مادامت الجريمة - التهديد - قد وقعت متكاملة الأركان في تاريخ سابق على ذلك القضاء بالبراءة⁽¹⁾. ويتضح من ذلك أن المشرع القطري قد نص على التجريم ليشمل التهديد أو الابتزاز الإلكتروني لمقطع فيديو أو صورة حقيقية أو مفبركة؛ أي تم تزييفها؛ سواء تم هذا التزييف بالطرق التقليدية أم عبر تقنيات وأنظمة الذكاء الاصطناعي.

علاوة على ما سبق؛ فقد نص المشرع القطري في قانون حماية خصوصية البيانات الشخصية رقم 13 لسنة 2016، على حماية البيانات الشخصية والتي تشمل حماية بيانات هويته المحددة، أو التي يمكن تحديدها بصورة معقولة⁽²⁾، والتي تشمل حماية الحق في الصورة والصوت من أي صورة من صور الاعتداء عليها، ومنها التزييف العميق باستخدام تقنيات الذكاء

1 - محكمة التمييز القطرية، تمييز جنائي، جلسة 16 أكتوبر 2017، الطعن رقم 63 لسنة 2017.

2 - المادة الأولى من التعريفات من قانون حماية خصوصية البيانات الشخصية القطري رقم 13 لسنة 2016، والمنشور في الجريدة الرسمية رقم 15، والصادرة بتاريخ 29 ديسمبر 2016، ص 3.

الاصطناعي. وبالرغم مما سبق؛ نستطيع القول بأن المشرع القطري لم ينص صراحة على قواعد خاصة لتجريم التزييف العميق باستخدام تقنيات الذكاء الاصطناعي، وبالتالي ندعو المشرع إلى ضرورة التدخل للنص على قواعد خاصة لمواجهة جرائم التزييف العميق باستخدام تقنيات الذكاء الاصطناعي وذلك لخطورتها على أمن وسلامة المجتمع والأفراد، وفي نفس الوقت واختلاف جريمة التزييف العميق باستخدام أنظمة الذكاء الاصطناعي على الصورة التقليدية من التزييف والتزوير الذي يجرم وفقا للقواعد القانونية التقليدية في القوانين الجنائية، وهذا ما سوف نتناوله بالشرح في الفرع الثاني.

ثالثا: خصائص التزييف العميق باستخدام تقنيات الذكاء الاصطناعي:

تتنوع وتتعدد الخصائص التي تتميز بها ظاهرة التزييف العميق باستخدام تقنيات الذكاء الاصطناعي، وذلك ما سوف نستعرضه على النحو التالي⁽¹⁾:

1 - درجة الخطورة الإجرامية العالية لظاهرة التزييف العميق باستخدام تقنيات الذكاء الاصطناعي على أمن واستقرار المجتمع؛ فمما لا شك فيه أن المعلومات والبيانات المزيفة تزييفا عميقا باستخدام خوارزميات أنظمة الذكاء الاصطناعي لها تأثير خطير على أمن وسلامة المجتمع واستقراره، بل أصبحت تشكل مادة أساسية لحروب الجيل الخامس من خلال نشر الشائعات والبيانات والمعلومات المضللة. وتطبيقا لذلك؛ نجد أن شركة (Sensity) للتكنولوجيا قد رصدت ارتفاعا ملحوظا لمقاطع الفيديو المزيفة تزييفا عميقا على شبكة الإنترنت في عام 2021⁽²⁾؛ مما يبرز خطورة انتشار ظاهرة التزييف العميق بواسطة خوارزميات أنظمة الذكاء

1 -Wilkerson, Lindsey, The rising concerns of deepfake technology and it influence on democracy and the first amendment, Missouri Law, Review, 2021, Vol, 86, (1).

2 - هذا ما أكد عليه معهد الأمم المتحدة لبحوث نزع السلاح (UNIDIR) في تقريره بشأن تداعيات الابتكارات التكنولوجية للذكاء الاصطناعي على الخصوصية الرقمية والأمن والثقة، خاصة ظاهرة التزييف العميق والثقة والأمن الدولي، في 25 أغسطس 2021، جنيف؛ ففي هذا التقرير تم رصد ارتفاع ظاهرة التزييف العميق باستخدام تقنيات الذكاء الاصطناعي وانتشار مقاطع الفيديو والصور المزيفة تزييفا عميقا خاصة على مواقع التواصل الاجتماعي الإلكترونية وعلى التطبيقات الإلكترونية والمراسلة والشات؛ مما يمثل معه خطورة على الحق في الخصوصية الرقمية ويهدد الأمن القومي للدول.

الاصطناعي خاصة من خلال مشاركتها على نطاق واسع عبر منصات التواصل الاجتماعي الإلكترونية وتطبيقات التراسل الإلكترونية عبر الإنترنت.

2 - الآثار الوخيمة لظاهرة التزييف العميق باستخدام تقنيات الذكاء الاصطناعي على صناعة الإعلام؛ حيث تمثل ظاهرة التزييف العميق تهديدا لصناعة الإعلام وخدمات تقنيات الوسائط المتعددة؛ نظرا لتطور أنظمة الذكاء الاصطناعي في العصر الحالي الأمر الذي أدى إلى اصطناع وتركيب مقاطع الفيديو والصور المزيفة تزييفا عميقا بشكل تبدو حقيقية للشخص العادي على خلاف الواقع، الأمر الذي يجعل جمهور المشاهدين يتشكك في مصداقية وسائل الإعلام.

3 - خطورة ظاهرة التزييف العميق على التشكيك في مصداقية أدلة الإثبات الجنائي المعتمدة على المحتوى المرئي أو الصوتي؛ حيث تمثل ظاهرة التزييف العميق باستخدام تقنيات الذكاء الاصطناعي تهديدا حقيقيا على التشكيك في مصداقية أدلة التوثيق بالصوت والفيديو كأدلة إثبات جنائية أمام المحاكم، وتكمن خطورة التزييف العميق بواسطة خوارزميات أنظمة الذكاء الاصطناعي إلى وصوله لدرجة تجعل على الشخص الفني المختص صعوبة للتفرقة ما بين مقاطع الفيديو والصور المزيفة تزييفا عميقا وتلك الفيديوهات والصور الحقيقية، وبالتالي أصبح الاعتقاد القائم على أن التوثيق بالصوت والفيديو دليل يتمتع بالمصداقية في المعلومات والبيانات اعتقاد يعتره الشك، ولا يمكن الاعتماد عليه بشكل كامل في الإثبات الجنائي كقرينة قاطعة.

وتطبيقا على ذلك؛ فقد أثير في الولايات المتحدة الأمريكية تساؤل حول ما مدى دقة تقارير خبراء الطب الشرعي للوسائط الرقمية أمام المحكمة الفيدرالية الأمريكية بشأن توثيق

انظر: الموقع الإلكتروني:

<https://documents-dds-ny.un.org/doc/unidir.innovations-dialogue.com>

تاريخ زيارة الموقع الإلكتروني 31 أغسطس 2024.

الأدلة في حالة ما إذا كان هناك تزييف عميق لهذه الوسائط الرقمية، خاصة في ظل عدم وجود تقنية قاطعة بشأن الكشف عن التزييف لدى خبراء الطب الشرعي للوسائط الرقمية⁽¹⁾. وبناء على ذلك تظهر أهمية التنظيم القانوني الخاص لمواجهة هذه الظاهرة الإجرامية لما تمثله من مخاطر جمة على أدلة الإثبات للوسائط الرقمية أمام المحاكم الجنائية.

4 - من الجرائم التي تعتمد على التكنولوجيا المستحدثة وتقنيات أنظمة الذكاء الاصطناعي، في واقع الأمر إن ظاهرة التزييف العميق باستخدام تقنيات الذكاء الاصطناعي أدت إلى إمداد المجرمين بقدرات فائقة تمكنهم من ارتكاب الجرائم الإلكترونية من خلال الاستعانة بالقدرات التكنولوجية المتطورة بشكل هائل في مجال أنظمة الذكاء الاصطناعي، وبالتالي تهديد الأمن العام للمجتمع وأمن وسلامة الأفراد؛ حيث يتطلب هذا النوع من الجرائم تمكن الجناة من المهارات التكنولوجية وتقنيات أنظمة الذكاء الاصطناعي، والقدرة على التعامل مع البرامج والأجهزة الإلكترونية. فمن أجل ارتكاب جرائم التزييف العميق بجودة عالية يتطلب ذلك توفر مهارات تقنية وبرامج وأجهزة إلكترونية مناسبة تمكن المجرمين من التزييف العميق لكل من الصوت والصورة بشكل محترف وبجودة عالية.

5 - تعتبر جريمة التزييف العميق باستخدام أنظمة الذكاء الاصطناعي من الجرائم التي تؤثر على الرأي العام عبر نشر الشائعات والأخبار الكاذبة والمضللة؛ فمما لا شك فيه أن جرائم التزييف العميق باستخدام خوارزميات الذكاء الاصطناعي لها تأثير خطير على العملية الديمقراطية؛ خاصة في مرحلة الدعاية الانتخابية وذلك من حيث قدرتها على تشوية سمعة الأشخاص السياسيين عن طريق الإسناد الخاطئ لوقائع غير حقيقية لهم؛ مما يساهم في إضعاف الثقة فيهم وخداع وتضليل جمهور الناخبين⁽²⁾؛ مما يؤثر على توجهات جمهور

1 - Maras, Marie Helen, Alexandrou Alex, Determining authenticity of video evidence in the age of artificial intelligence and in the wake of deepfake videos, the international journal of evidence & proof, 2019, Vol, 23 (3).

2 - Diakopoulos Nicholas, Johnson Deborah, Anticipating and addressing the ethical implications of deepfakes in the context of elections, New media & Society, 2021, Vol, 23, (7).

الناخبين. وتطبيقاً على ذلك؛ فقد أكدت الدراسات التي قام بها العلماء (Wilkerson, Wang, Patrini, Ajder)، في الفترة ما بين عام 2019 إلى 2021 إلى أن نسبة 96% من إجمالي مقاطع الفيديو المزيفة بتقنية التزييف العميق باستخدام تقنيات الذكاء الاصطناعي كانت عبارة عن اصطناع فيديوهات إباحية جنسية لأشخاص سياسيين أو معروفين من أجل تصفيتهم معنويًا، أو تشويه سمعتهم، أو الانتقام الإباحي منهم، أو ابتزازهم ماليًا أو جنسيًا⁽¹⁾، أو من خلال اصطناع فيديوهات مزيفة تتضمن بيانات ومعلومات كاذبة من أجل نشرها لتضليل الأفراد؛ لتحقيق فوز في المجتمع، أو الاحتيال المالي، أو إفساد الحياة الديمقراطية عن طريق تضليل الناخبين، أو افتعال الأزمات الدبلوماسية بين الدول⁽²⁾.

6 - دقة جودة المحتوى المرئي والصوت لمقاطع الفيديو والصور الناتج عن عمليات التزييف العميق باستخدام خوارزميات أنظمة الذكاء الاصطناعي؛ بحيث لا تظهر أي تشويش أو تغير في اللون أو التعرض المفرط. فالتزييف العميق باستخدام تقنيات الذكاء الاصطناعي يجعل الشخص العادي يعتقد بحقيقة مقاطع الفيديو والصور والصوت المزيفة؛ حيث تتيح عملية التزييف العميق تأثير على الشخص العادي متوسط الخبرة والذكاء بأن الفيديو حقيقي على خلاف الواقع.

الفرع الثاني

صور التزييف العميق باستخدام تقنيات الذكاء الاصطناعي والتفرقة بينها وبين التزييف التقليدي

تتعدد صور التزييف العميق باستخدام تقنيات وأنظمة الذكاء الاصطناعي، وبالتالي سوف نستعرض في البداية لصور التزييف العميق باستخدام تقنيات الذكاء الاصطناعي "أولاً"، ثم

- 1 - Wang S., Kim S., User's emotional and behavioral responses to deepfake videos of k-pop idols, computers in human behavior, site V. 30/08/2023: <https://doi-org/10.1016/j.chb.2022.107305>.
- 2 - Ajder H., Patrini G., at, The state of deepfakes: landscape, threats, and impact, Amsterdam, 2019, Deeptrace, site V. 30/08/2024: <http://regmedia.co.uk/2019/10/08/deepfake-report.pdf>.

بعد ذلك تتناول التفرقة ما بين التزييف التقليدي والتزييف العميق باستخدام تقنيات الذكاء الاصطناعي "ثانياً"، وذلك على النحو التالي:

أولاً: صور التزييف العميق باستخدام تقنيات الذكاء الاصطناعي:

قبل أن نتناول صور التزييف العميق باستخدام تقنيات الذكاء الاصطناعي، نوضح أنواع أنظمة الذكاء الاصطناعي؛ فقد نصت المادة 52 من مشروع قانون الذكاء الاصطناعي في فرنسا على ثلاثة أنواع لأنظمة الذكاء الاصطناعي؛ سواء كانت عالية الخطورة أم لا، وهي على النحو التالي⁽¹⁾:

النوع الأول: أنظمة الذكاء الاصطناعي التفاعلية؛ حيث إن هذا النوع من أنواع أنظمة الذكاء الاصطناعي يقوم على أساس التفاعل مع الأشخاص الطبيعيين باستخدام الروبوتات الذكية وأنظمة الذكاء الاصطناعية التفاعلية الأخرى.

النوع الثاني: أنظمة الذكاء الاصطناعي التعبيرية؛ حيث إن هذا النوع من أنواع أنظمة الذكاء الاصطناعي تهدف إلى التعرف على مشاعر التصنيف البيومترية من خلال تقنيات وأنظمة الذكاء الاصطناعي.

النوع الثالث: أنظمة الذكاء الاصطناعي البحثية، وهذا النوع من أنظمة الذكاء الاصطناعي يتعلق بالنشاط البحثي وهو ما يطلق عليه التزييف العميق باستخدام تقنيات الذكاء الاصطناعي؛ حيث يتم التلاعب في الصورة أو الصوت أو مقاطع الفيديو لجعلها مشابهة للأشخاص الحقيقيين أو الأشياء أو الكيانات أو الأحداث الأخرى من أجل إنشاء محتوى يبدو على خلاف الواقع حقيقياً. ويجوز استخدام التزييف العميق كضرورة لممارسة الحق في حرية التعبير أو الحق في حرية الفنون والعلوم، ولكن في هذه الحالة ومن أجل ضمان مشروعية هذه الأفعال، لا بد وأن يلزم

1 - انظر: مشروع قانون الذكاء الاصطناعي في فرنسا، المادة 25 منه، وذلك على الرابط الإلكتروني:

www.legifrance.gouv.fr

تاريخ الزيارة 2024/11/12.

المشرع المطورين ومستخدمي الأعمال والجهات الفاعلة الأخرى في سلاسل قيمة الإدارية، بما يلي⁽¹⁾:

أ - يجب الالتزام بإعلام الأشخاص بأن المحتوى قد تم إنشاؤه أو التلاعب به بشكل مصطنع، في ضوء الالتزام بالحق في الإعلام والتبصير عن طريق تقديم كافة الضمانات المناسبة لحماية حقوق وحريات الأشخاص.

ب - أن يتم ذلك كضرورة من أجل ممارسة الحق في حرية التعبير أو الحق في حرية الفنون والعلوم.

ج - لا يجوز تطبيق هذه الالتزامات على أنظمة الذكاء الاصطناعي التي يسمح بها القانون والتي تهدف إلى الكشف عن الجرائم الجنائية ومنعها والتحقق فيها لمقاضاة مرتكبيها.

وتطبيقاً على ذلك؛ فقد نص المشروع الأوروبي في لائحة الخدمات الرقمية على مواجهة التزييف العميق باستخدام تقنيات الذكاء الاصطناعي إلى أن عدم الامتثال لأي شرط أو التزام بخلاف ما هو منصوص عليه سابقاً يعاقب بعقوبة الغرامة المالية التي تصل إلى 20 مليون يورو، أو إذا كان الجاني شخصاً اعتبارياً تكون مقدار الغرامة 4% من إجمالي مبيعاته السنوية للسنة المالية السابقة على ارتكاب الجريمة أو 20 مليون يورو أيهما أعلى، ويكون مقدار الغرامة المالية للمؤسسات والوكالات والهيئات التابعة للاتحاد الأوروبي 250,000 ألف يورو.

أما بالنسبة لصور التزييف العميق باستخدام تقنيات الذكاء الاصطناعي؛ فنستطيع تقسيم صور التزييف العميق إلى العديد من الأنواع، وذلك حسب كل معيار للتقسيم، وذلك على النحو التالي:

المعيار الأول لصور التزييف العميق باستخدام تقنيات الذكاء الاصطناعي؛ حيث ينقسم

1 - Cécile Crichton, Projet de règlement sur l'IA (II): une approche fondée sur les risques, Dalloz actualité 04 mai 2021, Sit: [https:// www.dalloz.fr/ documentation/ Document?ctxt=0_YSR_0MD1](https://www.dalloz.fr/documentation/Document?ctxt=0_YSR_0MD1)

التزييف العميق حسب معيار محل التزييف إلى ثلاثة أنواع: التزييف العميق للمحتوى المرئي، والتزييف العميق للمحتوى الصوتي، والتزييف العميق الفائق أو المتقدم، وذلك على النحو التالي:

1 - النوع الأول: التزييف العميق باستخدام تقنيات الذكاء الاصطناعي للمحتوى المرئي:

يتمثل هذا النوع من التزييف العميق باصطناع أو تركيب مقاطع فيديو أو صور مفبركة لشخص ما من خلال استخدام خوارزميات أنظمة الذكاء الاصطناعي على خلاف الواقع، مثال على ذلك، إنشاء مقاطع الفيديو والصور المزيفة للمشاهير وللأشخاص السياسيين من أجل ابتزازهم والتشهير بهم أو الإضرار بسمعتهم، وذلك عن طريق أما تبديل وجه الشخص المعني بواسطة خوارزميات الذكاء الاصطناعي؛ حيث يتم في هذه الحالة استبدال وجه شخص محدد من خلال تقنيات فك التشفير وتركيب الخرائط الرقمية للوجه باستخدام الخوارزميات التي تقوم بنفس حركات وتعبيرات وجه الشخص المراد تزييف صورته أو مقطع الفيديو الخاص به، ومثال على ذلك، مقطع الفيديو الشهير للرئيس الأمريكي الأسبق بارك أوباما؛ حيث قام فريق (Buzz Feed) بالاستعانة بأحد الممثلين ليقوم بعملية تقليد حركة وجه وفم بارك أوباما، ثم بعد ذلك بواسطة أحد التطبيقات الإلكترونية التي تعمل بتقنيات الذكاء الاصطناعي تمت عملية معالجة هذه المشاهد المصورة للممثل لتبدو صورة مقبولة لبارك أوباما، أما بالنسبة للصوت فتم الاستعانة بممثل آخر قام بتقليد صوت بارك أوباما وإيماءاته⁽¹⁾، وفي النهاية ظهر الفيديو المفبرك بصورة تبدو حقيقية بدرجة مرعبة بعد عمليات التزييف العميق باستخدام خوارزميات تقنيات الذكاء الاصطناعي.

أما الحالة الثانية؛ فيتم تزييف المحتوى المرئي تزييفا عميقا من خلال استخدام تقنيات

1 - د. ليليا بوسحرة، د. عبد القادر بودربالة، التزييف العميق والدعاية الرقمية في عصر التمكين الرقمي: قراءة في النماذج والرهانات، مجلة مصداقية، المدرسة العليا العسكرية للإعلام والاتصال، مجلد 5، عدد 1، الجزائر، 2023، ص 31.

الشبكات التوليدية التنافسية لأنظمة الذكاء الاصطناعي؛ لتغيير ملامح الوجه فقط من خلال تعديل تعبيرات الوجه للشخص المعني ومزامنة ذلك مع حركة الشفاه⁽¹⁾؛ بحيث يتم إدخال البيانات المزيفة على حركة الشفاه الحقيقية للشخص المعني، ومثال على ذلك، الصور المصطنعة ضمن سلسلة من مجموعة الصور الحقيقية للشخص المعني بشكل تبدو فيها حقيقية وذلك باستخدام تقنيات الشبكات التوليدية التنافسية لأنظمة الذكاء الاصطناعي.

2 - النوع الثاني: التزييف العميق باستخدام تقنيات الذكاء الاصطناعي للمحتوى الصوتي:

يقوم هذا النوع من التزييف العميق باستخدام أنظمة الذكاء الاصطناعي؛ لتقليد الصوت بطريقة التحكم في نبرة صوت شخص ما تجعل الطرف الآخر الذي يستمع للمحتوى الصوتي يعتقد بأنه الصوت الحقيقي، أو تركيب الصوت وتعديله وذلك عن طريق استحداث ملف صوتي مزيف على خلاف الحقيقة، ومثال على ذلك، في عام 2019 تعرضت شركة ألمانية للطاقة للاحتيال بمبلغ 220 ألف دولار بعد أن تم اصطناع محتوى صوتي مزيف تزييفا عميقا باستخدام تقنيات الذكاء الاصطناعي لصوت شخصية تنفيذية رفيعة المستوى للشركة يطلب فيه من الموظف القيام بعملية التحويل المالي الفوري للمبلغ⁽²⁾؛ حيث إن المحتوى الصوتي المزيف تزييفا عميقا كان قادرا على تقليد الصوت والنغمة وعلامات التوقف الصوتية واللهجة الألمانية بشكل مثالي يدعو للقلق من دقة التزييف للصوت.

3 - النوع الثالث: التزييف العميق الفائق باستخدام تقنيات الذكاء الاصطناعي بناء على سلوك الشخص (Hyper faking) وتوقع تصرفاته في المستقبل

يرتكب الجناة هذا النوع من التزييف العميق من خلال إنشاء محتوى مصطنع عن شخص

1 - د. ليليا بوسحرة، د. عبد القادر بودريالة، المرجع السابق، ص 32.

2 - أ. معين الميتمي، التزييف العميق، مستقبل القوانين المنظمة للبرمجيات الذكية، وذلك على الموقع الإلكتروني: <http://al-ain.com/article/deepfake-the-future-of-smart-software-law>

تاريخ الزيارة 2 سبتمبر 2024.

ما بناء على سلوك الشخص المصدر، أو إنشاء محتوى مشابه بشكل مصطنع بناء على أوامر نصية؛ فيتم استغلال تقنيات الذكاء الاصطناعي في عملية تغيير الحقيقة بهدف الإضرار بالأشخاص؛ مما يؤثر على النظام العام في الدول، ومثال على ذلك التزييف العميق من خلال شبكات الميتافيرس أو من خلال تطبيق (CHATGPT).

المعيار الثاني لصور التزييف العميق باستخدام تقنيات الذكاء الاصطناعي معيار الغاية؛ حيث ينقسم التزييف العميق حسب معيار الغاية إلى ما يلي:

1 - النوع الأول: التزييف العميق باستخدام تقنيات الذكاء الاصطناعي من أجل الانتقام الإباحي؛ حيث ترجع أسباب انتشار ظاهرة التزييف العميق باستخدام تقنيات الذكاء الاصطناعي لاستغلاله في الانتقام الجنسي أو الإباحي لشخص معين من أجل تهديده وابتزازه والتشهير به، لذلك فقد سعت العديد من التشريعات المقارنة على تجريم هذه الصورة من صور التزييف، ومثال على ذلك، في إحدى الولايات الأمريكية ولاية كاليفورنيا في عام 2019 تم اقتراح مشروع قانون لتجريم التزييف العميق من أجل الانتقام الإباحي، وكذلك المشرع البريطاني والمشرع الفرنسي اقترحا نصوص قانونية لتجريم هذا النوع من جرائم التزييف العميق باستخدام تقنيات الذكاء الاصطناعي.

2 - النوع الثاني: التزييف العميق باستخدام تقنيات الذكاء الاصطناعي من أجل تشويه السمعة والتشهير خاصة في المجال السياسي والفني، ويتمثل خطورة هذا النوع من التزييف العميق باستخدام تقنيات الذكاء الاصطناعي في التأثير على الرأي العام والديمقراطية في الدول؛ لذلك فقد سعى المشرع الأوروبي إلى وضع لائحة أوروبية للذكاء الاصطناعي؛ حيث تم اعتماد القراءة الأولى لمشروع هذه اللائحة في 14 يونيو 2023، وصدرت في 13 يونيو 2024 اللائحة الأوروبية بشأن الذكاء رقم 1689 لسنة 2024، ودخلت بعض قواعدها حيز النفاذ في الأول من أغسطس 2024⁽¹⁾.

1 - انظر: المادة 50 من اللائحة الأوروبية بشأن الذكاء الاصطناعي رقم 1689 لسنة 2024، والصادرة في 13 يونيو 2024، وقد دخلت بعض قواعدها حيز النفاذ في الثاني من أغسطس 2024.

3 - النوع الثالث: التزييف العميق باستخدام تقنيات الذكاء الاصطناعي لأدلة الوسائط الرقمية المعتمد عليها في الإثبات الجنائي؛ حيث يتمثل خطورة هذا النوع من التزييف العميق في تأثيره الخطير على العدالة والتشكيك في مصداقية الأحكام القضائية التي تعتمد على الأدلة للوسائط الرقمية ذات المحتوى المرئي أو الصوت المحتمل أن يكون قد تم تزييفه تزييفا عميقا باستخدام خوارزميات أنظمة الذكاء الاصطناعي.

ثانيا: التفرقة ما بين التزييف العميق باستخدام تقنيات الذكاء الاصطناعي والتزييف التقليدي:

يقصد بالتزييف بشكل عام بأنه: "إعادة إنتاج أو إعادة تقديم لعمل ما بطريقة غير مشروعة"⁽¹⁾. وبناء على ذلك نستطيع القول بأن التزييف العميق باستخدام تقنيات الذكاء الاصطناعي يعتبر مرادف للتزييف الإلكتروني والذي يقصد به كل فعل من شأنه أن يغير الحقيقة في المحتوى الرقمي أو الإلكتروني؛ سواء كان في شكل محتوى مرئي أم صوت أم دعائم وسائط إلكترونية تشمل بيانات ومعلومات تم معالجتها آليا بواسطة تقنيات الذكاء الاصطناعي، وذلك متى توفرت لدى الفاعل نية استعمالها فيما زيف أو زور من أجله.

أما بالنسبة لتعريف التزييف التقليدي فيقصد به كل فعل يغير الحقيقة في مستند أو محرر من شأنه أن يجعل الشيء المفبرك يظهر بمظهر حقيقي يخالف الواقع، ومثال على ذلك، التمويه الذي يقوم به الجاني على عملة بطلاء يجعلها شبيهة بعملة أخرى أكثر منها قيمة أو تغيير الحقيقة في محرر على خلاف الحقيقة أو اصطناعه من الأساس، والتزوير الذي يتم على محرر فيغير الحقيقة فيه عن طريق الاصطناع أو التقليد. وتطبيقا على ذلك؛ فقد جرى قضاء محكمة النقض المصرية في جرائم التزييف التقليدية على أن تحضير الأدوات والسبائك اللازمة للتزييف واستعمالها بالفعل في إعداد العملة المزيفة التي لم تصل إلى درجة من الإتقان تكفل

1 - د. أحمد محمد فتحي الخولي، المسؤولية المدنية الناتجة عن الاستخدام غير المشروع لتطبيقات الذكاء الاصطناعي «الديب فيك نموذجاً»، مجلة البحوث الفقهية والقانونية، العدد 36، إصدار أكتوبر 2021، ص 250.

لها الرواج في المعاملة هو في نظر القانون من أعمال الشروع المعاقب عليه قانوناً؛ حيث إن الجناة قد تعدوا مرحلة الأعمال التحضيرية وانتقلوا إلى مرحلة بدء التنفيذ بحيث لو تركوا وشأنهم لتمت الجريمة في أعقاب ذلك مباشرة⁽¹⁾، ويلاحظ أن المشرع قد مد الحماية القانونية من جريمة التزييف فعاقب على مجرد الشروع في ارتكابها.

ويتضح مما سبق أن جريمة التزييف العميق باستخدام خوارزميات أنظمة الذكاء الاصطناعي تختلف عن جريمة التزييف التقليدية في أن جريمة التزييف العميق تتميز بأنها سهلة الارتكاب وذلك نتيجة استخدام تقنيات الذكاء الاصطناعي والتعلم الآلي بما يوفر على الجناة سهولة في ارتكاب هذا النوع من الجرائم على عكس جرائم التزييف التقليدية التي تتطلب من الجناة مهارة وحرافية عالية في التزييف والتزوير للمحركات والمستندات حتى يستطيع ارتكاب الجريمة؛ حيث تتميز بالصعوبة في طريقة ارتكابها. علاوة على ذلك؛ فإن مرتكبي جريمة التزييف العميق باستخدام خوارزميات الذكاء الاصطناعي يتمتعون بالذكاء والقدرة على التعامل مع تقنيات وأنظمة الذكاء الاصطناعي وبرامج معالجة البيانات والمعلومات الإلكترونية على عكس الجناة مرتكبي جرائم التزييف والتزوير التقليدية؛ مما يجعل من الصعوبة معه اكتشاف التزييف في جرائم التزييف العميق باستخدام تقنيات الذكاء الاصطناعي؛ نظراً لاستخدام مستوى احترافي من التكنولوجيا وخوارزميات الذكاء الاصطناعي في معالجة المحتوى الرقمي بدرجة من التعقيد تجعل من الصعوبة بالأمر الكشف على عملية التزييف. علاوة على ذلك؛ فإن الآثار المترتبة على جرائم التزييف العميق باستخدام خوارزميات الذكاء الاصطناعي ليست محدودة النطاق⁽²⁾؛ حيث تمتد آثارها إلى نطاق عابر للحدود الوطنية على عكس جريمة التزييف التقليدية التي غالباً ما تكون آثارها مقتصرة على نطاق جغرافي محصور في الدول محل ارتكاب الجريمة فيها.

1 - محكمة النقض المصرية، نقض جنائي، جلسة 8 ديسمبر 1964، الطعن رقم 331 سنة 34 ق، السنة 15، ص 795. وكذلك نقض جنائي جلسة 28 يونيو 1965 طعن رقم 144 سنة 35 ق، السنة 16، ص 361. وكذلك نقض جنائي، جلسة 4 أبريل 1976، الطعن رقم 1526 لسنة 45 ق، السنة 27، ص 386.

2 - د. جواحي عبد الستار، جرائم الحاسوب، دراسة مقارنة بين الشريعة الإسلامية والقانون الجزائري، مذكرة تخرج لنيل شهادة الماجستير في العلوم الإسلامية، قسم العلوم الإنسانية، كلية العلوم الاجتماعية والإنسانية، جامعة الشهيد حمه لخضر، الجزائر، 2015.

بالإضافة إلى ذلك؛ فإن المشرعين المصري والقطري يشترطان لقيام جريمة التزييف التقليدية توفر قصد جنائي خاص يتمثل في نية استعمال العملة المزيفة؛ علاوة على القصد الجنائي العام المتمثل في توفر عنصري العلم والإرادة، وتطبيقا على ذلك؛ فقد قضت محكمة النقض المصرية بأن جريمة التزييف وإن استلزمت - فضلا عن القصد الجنائي العام - قصدا خاصا - هو نية استعمال العملة المزيفة في التداول؛ مما يتعين على الحكم استظهاره إلا أن المحكمة لا تلتزم بإثباته في حكمها على استقلال متى كان ما أوردته عن تحقيق الفعل المادي يكشف بذاته عن توفر تلك النية التي يتطلبها القانون، وذلك ما لم تكن محل منازعة من الجانبين فإنه يكون متعيينا حينئذ على الحكم بيانها صراحة وإيراد الدليل على توفر نية استعمال العملة المزيفة⁽¹⁾. وتأسيسا على ما سبق؛ نستطيع القول بأن جريمة التزييف العميق باستخدام تقنيات الذكاء الاصطناعي تختلف بشكل واضح عن جريمة التزييف التقليدية المتعارف عليها وفقا لقواعد قانون العقوبات، الأمر الذي يستوجب معه استحداث قواعد قانونية خاصة لمكافحة هذه النوع من الجرائم، بحيث تتلاءم مع طبيعتها وخصائصها المتطورة والحديثة وتستهدف الجناة مرتكبي جرائم التزييف العميق باستخدام أنظمة الذكاء الاصطناعي.

المطلب الثاني

أركان جريمة التزييف العميق باستخدام تقنيات الذكاء الاصطناعي

مما لا شك فيه أن مقاطع الفيديو عبر الإنترنت وخاصة على مواقع التواصل الاجتماعي عبر الإنترنت والتطبيقات الإلكترونية أصبحت اليوم أداة مهمة لجذب جمهور المشاهدين من رواد المنصات الإلكترونية، بل تعدت الوسائل والأساليب التي تعمل على سرعة انتشارها عبر الإنترنت باعتبارها نوعا من الترفيه والتعليم، ولكن أساء بعض الأشخاص استخدام مقاطع الفيديو والصور لتشويه سمعة الغير من السياسيين أو الفنانين أو غيرهم من الأشخاص

1 - محكمة النقض المصرية، نقض جنائي، جلسة 18 أكتوبر 1965، الطعن رقم 34 ق السنة 16، ص 710.

العاديين، أو استخدامها في الأعمال المنافية للآداب العامة عن طريق اصطناعي أو تركيب الفيديوهات المفبركة غير الحقيقة عبر التزييف العميق باستخدام تقنيات الذكاء الاصطناعي. وبناء على ذلك؛ فسوف نستعرض في هذا المطلب البيان القانوني لجريمة التزييف العميق باستخدام تقنيات الذكاء الاصطناعي من خلال ما يلي، في الفرع الأول نتناول – بالتوضيح – الركن المادي لجريمة التزييف العميق باستخدام الذكاء الاصطناعي، وفي الفرع الثاني نستعرض الركن المعنوي لجريمة التزييف العميق باستخدام الذكاء الاصطناعي، وفي النهاية نتناول في الفرع الثالث – بالعرض – الآليات القانونية الجنائية لمواجهة جريمة التزييف العميق باستخدام الذكاء الاصطناعي.

الفرع الأول

الركن المادي لجريمة التزييف العميق باستخدام الذكاء الاصطناعي

تقوم جريمة التزييف العميق باستخدام الذكاء الاصطناعي على أساس التلاعب بمقاطع الفيديو والصور والصوت بكل إجراء من شأنه التلاعب في المحتوى المرئي أو الصوتي أو كليهما باستخدام تقنيات الذكاء الاصطناعي، وذلك من أجل تزييف حقيقة الأشياء والأماكن أو الأشخاص وغيرها من البيانات والمعلومات الأخرى؛ بحيث يبدو المحتوى المزيف تزييفا عميقا باستخدام خوارزميات الذكاء الاصطناعي حقيقيا للشخص المعتاد متوسط الخبرة والمعرفة. وبناء على ذلك نستطيع القول بأن محل جريمة التزييف العميق باستخدام الذكاء الاصطناعي يقع على المحتوى المزيف سواء كان المحتوى المزيف مرئيا أم صوتيا، وكذلك نستطيع القول بأن الركن المادي لجريمة التزييف العميق باستخدام تقنيات الذكاء الاصطناعي يتم من خلال ارتكاب صورة من صور الأنشطة الإجرامية التي تتمثل في اصطناع أو تركيب أو إنشاء من أجل تزييف المحتوى المرئي أو الصوتي، وذلك على النحو التالي:

أولاً: تزييف المحتوى المرئي باستخدام تقنيات الذكاء الاصطناعي في صورة تغيير الحقيقة من خلال (التركيب - الاصطناع - الإنشاء):

حيث يتم في هذه الحالة استخدام تقنيات الذكاء الاصطناعي في إنشاء محتوى مزيف تزييفا عميقا يتمثل في صور أو مقاطع الفيديو مزيفة تزييفا عميقا، ويتم هذا السلوك الإجرامي من خلال تغيير الحقيقة في المحتوى بأحدى الصور التالية⁽¹⁾:

الحالة الأولى: تزييف المحتوى المرئي عن طريق تغيير الوجه باستخدام خوارزميات أنظمة الذكاء الاصطناعي بواسطة فك التشفير والتشفير لوجه الشخص محل جريمة التزييف المرئي لوضعها على وجه شخص آخر، وذلك بواسطة معرفة تركيب الخريطة الرقمية لمقطع الفيديو أو الصور المراد تزييفها تزييفا عميقا باستخدام تقنيات الذكاء الاصطناعي. وفي هذه الحالة يتم تغذية تطبيق الذكاء الاصطناعي بالعديد من الصور الحقيقية للشخص محل جريمة التزييف العميق والشخص القائم بعملية التزييف من أجل كشف أوجه التشابه والاختلاف بينهما، وبناء على ذلك تقوم خوارزميات الذكاء الاصطناعي بعمليات المعالجة للبيانات والمعلومات لمقاطع الفيديو والصور والتي ينتج عنها المحتوى المرئي المزيف لمقاطع الفيديو والصور.

الحالة الثانية: تزييف المحتوى المرئي عن طريق التلاعب بالوجه باستخدام تقنيات الذكاء الاصطناعي؛ حيث يتم تعديل تعابير الشخص محل عملية التزييف العميق ومزامنة حركات الشفاه باستخدام خوارزميات الذكاء الاصطناعي بواسطة الشبكات التوليدية التنافسية، ففي هذه الحالة يتم إدخال بيانات كم من المعلومات والبيانات في تقنية الخوارزميات الذكاء الاصطناعي من أجل القيام بتحويلها إلى صور ومقاطع فيديو بواسطة تقنية الشبكات التوليدية التنافسية، عقب ذلك يتم إضافة الصور ومقاطع الفيديو المصنوعة إلى سلسلة الصور ومقاطع الفيديو الحقيقية للشخص محل عملية التزييف العميق، وبناء على ذلك تقوم تقنية الخوارزميات

1 - انظر: دليل التزييف العميق، البرنامج الوطني للذكاء الاصطناعي، دولة الإمارات العربية المتحدة، يوليو 2021، ص 10، 11.

لأنظمة الذكاء الاصطناعي بتحسين جودة عمليات معالجة هذه المعلومات والبيانات؛ مما يؤدي في النهاية إلى التوصل إلى مقاطع الفيديو والصور المزيفة تزييفا عميقا التي تبدو حقيقية على خلاف الواقع.

ثانيا: تزييف المحتوى الصوتي عن طريق تغيير الحقيقة باستخدام تقنيات الذكاء الاصطناعي:

حيث يتم في هذه الحالة تزييف المحتوى الصوتي تزييفا عميقا باستخدام تقنيات الذكاء الاصطناعي عن طريق تركيب الصوت وتعديله من خلال إنشاء ملف صوتي مزيف يتضمن نفس صوت الشخص محل جريمة التزييف العميق ولكن لكلام لم يقله في حقيقة الأمر، أو تغيير نبرة صوته للتلاعب بالحقائق من أجل إظهار قيامه بسلوك غير حقيقي؛ مما يعطي انطباعا مزيفا عنه يخالف حقيقة الأمر وبشكل يضر ويشوه سمعة الشخص محل التزييف العميق، ويتم بعد ذلك نشر هذه المقاطع المزيفة على مواقع التواصل الاجتماعي الإلكترونية وعلى المواقع الإخبارية عبر الإنترنت.

والنتيجة الإجرامية لجريمة التزييف العميق باستخدام خوارزميات الذكاء الاصطناعي تتمثل في نشر المحتوى المزيف للجمهور دون رضا الشخص المعني؛ حيث يستلزم للعقاب عن هذه الجريمة أن يكون المحتوى المزيف متاحا لعدد غير محدود من الأشخاص؛ مما يعني جعل المعلومات المفبركة سواء كانت في صورة مقاطع فيديو أم صور أو مقاطع صوتية متاحة بسهولة للمتلقي من الجمهور بشكل عام دون اتخاذ أي إجراء آخر من قبل المتلقي التي تقدم إليه هذا المحتوى المزيف، وبغض النظر عما إذا كان هؤلاء الأشخاص يصلون بالفعل إلى هذا المحتوى المزيف. علاوة على ضرورة توفر علاقة السببية بين السلوك الإجرامي المتمثل في توفر صورة من صور التزييف العميق باستخدام أنظمة الذكاء الاصطناعي والتي أدت إلى تحقق النتيجة الإجرامية المتمثل في التزييف العميق للفيديو أو الصوت ونشره على مواقع التواصل

الاجتماعي أو عبر الإنترنت أو التطبيقات الإلكترونية أو غيرها من الوسائل الرقمية والوسائط الإلكترونية المختلفة.

وبناء على ذلك؛ فقد نص المشرع الفرنسي في الفقرة الأولى من المادة 226 - 8 من قانون العقوبات على تجريم كل نشر بأي وسيلة كانت لصوت أو صورة تم التلاعب فيه عن طريق المونتاج دون موافقة الشخص المعني على ذلك، بحيث يعاقب بالسجن لمدة لا تزيد عن سنة وبالغرامة المالية التي لا يزيد مقدارها عن مبلغ 15.000 يورو⁽¹⁾. ولكن موقف المشرع الفرنسي محل انتقاد، وذلك لأن المشرع قصر التجريم عن طريق فعل المونتاج على الصوت أو الصورة، وبالتالي وكنتيجة لمبدأ الشرعية الجنائية لا يمكن التوسع في تفسير النص الجنائي ضد مصلحة المتهم بحيث يشمل التجريم الصور الحديثة للتزيف العميق باستخدام خوارزميات الذكاء الاصطناعي، وبناء على ذلك ففي 4 يوليو 2023 تم تقديم مشروع قانون يتعلق بتأمين وتنظيم الفضاء الرقمي إلى مجلس الشيوخ الفرنسي يهدف إلى مكافحة المحتوى غير القانوني عبر الإنترنت مثال: (مكافحة التحرش عبر الإنترنت - التحكم في عمر جمهور المحتوى الإباحي - تنظيم مواقع التأجير بغرض سياحي - تنظيم قضايا التغييرات في مشغلي العقود السحابية - مكافحة التزيف العميق باستخدام خوارزميات الذكاء الاصطناعي، ... إلخ)⁽²⁾.

وفيما يتعلق بوضع الإطار القانوني للتزيف العميق باستخدام خوارزميات الذكاء الاصطناعي؛ فقد اقترح مشروع القانون إضافة فقرة إلى المادة 226 - 8 من قانون العقوبات الفرنسي تنص على تجريم كل فعل من شأنه نشر لتلاعب أو تغيير الحقيقة بأي وسيلة كانت للمحتوى المرئي أو الصوتي الناتج عن المعالجة الخوارزمية وإعادة إنتاج صورة أو صوت كلمات لشخص ما، دون موافقته، ما لم يكن واضحا للشخص العادي أن المحتوى الصوتي أو

1 - La Code pénal française, Article 226-8, Modifié par Ordonnance n°2000-916 du 19 septembre 2000 - art. 3 (V) JORF 22 septembre 2000 en vigueur le 1er janvier 2002

2 - Sénat, Projet de loi, Sécuriser et réguler l'espace numérique, (1) ère lecture, PROCÉDURE ACCÉLÉRÉ, n° 778 , 777, 3 juillet 2023, Site:

https://www.senat.fr/amendements/2022-2023/778/Amdt_127.html, V., 11 sept 2024.

المرئي الذي تم إنشاؤه مفبرك من خلال تقنية التزييف العميق باستخدام خوارزميات الذكاء الاصطناعي، وفي هذه الحالة تكون العقوبة الحبس لمدة لا تزيد عن عام والغرامة المالية التي لا تزيد عن 15,000 يورو. بالإضافة إلى ذلك؛ فقد أضاف مشروع القانون فقرة تتعلق بتشديد العقوبة لتصبح السجن لمدة لا تزيد عن عامين والغرامة المالية التي لا يزيد مقدارها عن 45,000 يورو في حالة ما إذا تم نشر المحتوى المرئي أو الصوتي الناتج عن المعالجة الخوارزمية باستخدام خدمة اتصال عامة عبر الإنترنت.

وبموجب هذا النص تم تعريف التزييف العميق باستخدام تقنيات الذكاء الاصطناعي بأنه: تقنية تركيب أحادية أو متعددة الوسائط تعتمد على الذكاء الاصطناعي؛ بحيث يمكن استخدامه لتركيب أو دمج الصور أو ملفات الفيديو أو الصوت الموجودة على صور أو ملفات فيديو أو صوت، أو لإنشاء محتوى مصطنع حول شخص مستهدف بناء على سلوك الشخص المصدر، أو حتى من أجل إنشاء محتوى مشابه بشكل مصطنع بناء على أوامر نصية⁽¹⁾. وبناء على ذلك؛ فإن الواقع المعاصر يظهر منه الحاجة إلى ضرورة وضع إطار قانوني خاص للتعامل مع الإشكاليات القانونية التي تثيرها تقنيات الذكاء الاصطناعي وخاصة المتعلقة بالتزييف العميق باستخدام خوارزميات الذكاء الاصطناعي من أجل حماية الحقوق الرقمية للشخص خاصة حقه في خصوصية البيانات الشخصية والتي تتمثل في عدم استخدام بياناته الشخصية (الصوت والصورة) دون موافقته، وذلك عن طريق تغيير إرادة المشرع في ضوء السياسة التشريعية المعاصرة لمواجهة هذه الظاهرة الإجرامية الرقمية. علاوة على ذلك؛ حماية الحق في المعرفة وحرية تداول المعلومات للشخص في العالم الافتراضي كحماية للحقوق الرقمية للشخص، وعلى سبيل المثال لذلك؛ مكافحة التضليل الرقمي وانتشار الشائعات لحماية حق الجمهور في التمييز بين ما هو مفبرك وبين ما هو حقيقي من المعلومات والبيانات.

1 - Julie Groffe – Charrier, Vers un encadrement légal des deepfakes, le 12 juillet 2023, Dalloz Actualité, site:

https://www.dalloz-actualite.fr/flash/vers-un-encadrement-legal-des-deepfakes#results_box, V., Le 11 Sept 2023.

أما بالنسبة لموقف المشرع الأوروبي؛ فنجد أنه كان سابقا منذ عام 2017 في سعيه لوضع الإطار القانوني لأنظمة الذكاء الاصطناعي والروبوتات، وفي سبيل مواجهة المخاطر الناجمة عن استخدامات أنظمة الذكاء الاصطناعي؛ فقد سعى المشرع الأوروبي إلى وضع قانون للذكاء الاصطناعي؛ حيث تمت القراءة الأولى لمشروع اللائحة الأوروبية لتنظيم أنظمة الذكاء الاصطناعي في 14 يونيو 2023، وقد صدرت اللائحة الأوروبية بشأن الذكاء الاصطناعي في 13 يونيو 2024؛ حيث نصت المادة 50 من اللائحة الأوروبية بشأن الذكاء الاصطناعي رقم 1689 لسنة 2024 على مجموعة من الالتزامات بالشفافية التي تقع على عاتق الموردين والناشرين لأنظمة الذكاء الاصطناعي، منها ما يتعلق بمواجهة التزييف العميق باستخدام أنظمة الذكاء الاصطناعي، وهي على النحو التالي⁽¹⁾:

- 1 - الالتزام بوضع علامة يمكن قراءتها بوضوح على مخرجات أنظمة الذكاء الاصطناعي المخصصة للأغراض العامة والتي تولد محتوى اصطناعي من الصوت أو الصورة أو الفيديو أو النص، تفيد أنه مزيف أي ما تم إنشاؤه أو التلاعب بها بواسطة أنظمة الذكاء الاصطناعي غير حقيقي.
- 2 - الالتزام باحترام حق الأشخاص في الخصوصية وكافة القيود المنصوص عليها في الاتحاد الأوروبي لحماية الحق في الحياة الخاصة.
- 3 - الالتزام بإبلاغ الأشخاص المعرضين لأنظمة الذكاء الاصطناعي القادرة على التعرف على المشاعر أو نظم التصنيف البيومترية بتشغيل تلك الأنظمة وأنها تقوم بمعالجة البيانات الشخصية وفقا للوائح وقيود الاتحاد الأوروبي في حماية البيانات سواء الشخصية أم البيانات الأخرى، وفقا لللائحة الأوروبية رقم 679 لسنة 2016، واللائحة الأوروبية رقم 1725 لسنة 2018، والتوجيه الأوروبي رقم 680 لسنة 2018.

1 - انظر: المادة 50 من اللائحة الأوروبية بشأن الذكاء الاصطناعي رقم 1689 لسنة 2024، والصادرة في 13 يونيو 2024، ودخلت بعض قواعدها حيز النفاذ في الثاني من أغسطس 2024. الموقع الإلكتروني:

4 - التزام القائمين على نشر نظم الذكاء الاصطناعي بالإشارة إلى أن هذا النظام يقوم بإنشاء أو معالجة الصور أو محتوى الصوت أو الفيديو الذي يشكل تزيفاً عميقاً إلى أن المحتوى قد تم إنشاؤه أو معالجته بواسطة الذكاء الاصطناعي.

ويستثنى من هذه الالتزامات، عندما يكون الاستخدام مسموحاً به بموجب القانون لأغراض منع الجريمة، أو اكتشافها، أو التحقيق فيها، أو ملاحقة مرتكبيها قضائياً، أو عندما يكون المحتوى جزءاً من عمل، أو برنامج فني، أو إبداعي، أو ساخر، أو خيالي، أو ما شابه ذلك؛ فستمتع تلك الالتزامات بالشفافية بطريقة مناسبة لا تتعارض مع عرض العمل أو الاستمتاع به. ويتربط على الإخلال بتلك الالتزامات المتعلقة بالشفافية أن يتم توقيع عقوبة الغرامة المالية الإدارية التي تصل إلى 15 مليون يورو على القائمين بالنشر أو الموردين أو المشغلين لأنظمة الذكاء الاصطناعي أو نسبة 3% من إجمالي مبيعات الشركة السنوية في جميع أنحاء العالم أيهما أكبر⁽¹⁾.

الفرع الثاني

الركن المعنوي لجريمة التزييف العميق باستخدام الذكاء الاصطناعي

تعتبر جريمة التزييف العميق باستخدام تقنيات الذكاء الاصطناعي من الجرائم العمدية التي تتطلب توفر القصد الجنائي العام بعنصرية العلم والإرادة، بمعنى أن يعلم الجاني بأنه يقوم بإنشاء أو اصطناع أو تركيب مقطع فيديو أو صورة أو محتوى صوتي غير حقيقي للشخص المعني محل جريمة التزييف العميق وذلك باستخدام تقنية من تقنيات أنظمة الذكاء الاصطناعي، وأن إرادته الحرة والواعية قد اتجهت إلى ارتكاب هذا النشاط الإجرامي وإلى تحقيق النتيجة الإجرامية وهي تزييف الحقيقة في المحتوى الصوتي أو المرئي للشخص المعني بدن

1 - انظر: الفقرة الرابعة من المادة 99 من اللائحة الأوروبية بشأن الذكاء الاصطناعي رقم 1689 لسنة 2024، والصادرة في 13 يونيو 2024.

موافقته؛ أي جعل المحتوى يبدو حقيقيا على خلاف الواقع عن طريق تزييف الصوت أو الصورة أو الفيديو للشخص المعني، وأن يتم ارتكاب هذه الجريمة من أجل نشره دون موافقة أو رضا المجني عليه.

ويثور التساؤل حول هل جريمة التزييف العميق باستخدام تقنيات الذكاء الاصطناعي من الجرائم العمدية التي تتطلب بالإضافة إلى قصد جنائي عام توفر قصد جنائي خاص، أم أنه لا يشترط توفر القصد الجنائي الخاص للعقاب عن هذه الجريمة؟ وللإجابة على ذلك التساؤل نستطيع القول بأن جريمة التزييف العميق باستخدام تقنيات الذكاء الاصطناعي من الجرائم العمدية التي تتطلب قصد جنائي خاص يتمثل في نية استعمال المحتوى الصوتي أو المرئي المزيف تزييفا عميقا. حيث مناط الحماية في جريمة التزييف العميق يتمثل في حماية الحق في الصوت والصورة للشخص باعتبارها من الحقوق الأساسية للفرد، وبالتالي؛ فمن يقوم بارتكاب هذه الجريمة عن طريق إنشاء أو اصطناع أو تركيب أو التلاعب أو أي صورة أخرى من صور التزييف العميق باستخدام تقنيات الذكاء الاصطناعي، لا بد وأن يتوفر لديه نية خاصة تتمثل في نية استعمال هذا المحتوى المزيف فيما زيف من أجله، فعلى سبيل المثال إذا كان التزييف العميق من أجل الانتقام الجنسي أو الإباحي، فلا بد أن يتوفر لدى الجاني نية استعمال المحتوى المزيف تزييفا عميقا من أجل التشهير والانتقام الجنسي من المجني عليه عن طريق نشر هذه المقاطع المزيفة على المواقع الاجتماعية والمنتديات الإلكترونية وتطبيقات المراسلة الإلكترونية وغيرها من الصفحات والمواقع عبر الإنترنت.

الفرع الثالث

آليات المواجهة الجنائية للتزييف العميق باستخدام الذكاء الاصطناعي

سوف نستعرض في البداية آليات الكشف عن مقاطع الفيديو والصور والصوت المزيفة تزييفا عميقا باستخدام تقنيات الذكاء الاصطناعي (أولا)، ثم بعد ذلك نحدد آليات التعاون

الدولي في مكافحة جريمة التزييف العميق باستخدام خوارزميات الذكاء الاصطناعي (ثانياً)، عقب ذلك نوضح الضمانات الإجرائية واحترام حقوق الإنسان في جرائم التزييف العميق (ثالثاً)، وفي النهاية نستعرض التدابير الوقائية والاحترازية لمواجهة التزييف العميق باستخدام تقنيات الذكاء الاصطناعي (رابعاً)، وذلك على النحو التالي:

أولاً: آليات الكشف عن مقاطع الفيديو والصور والصوت المزيفة تزييفاً عميقاً باستخدام تقنيات الذكاء الاصطناعي:

في واقع الأمر؛ كما يمكن الاستعانة بخوارزميات الذكاء الاصطناعي من قبل الجناة في ارتكاب الجرائم وخاصة جريمة التزييف العميق، يمكن استخدام تقنيات الذكاء الاصطناعي والتعلم الآلي في الوقاية من الجرائم وخاصة جريمة التزييف العميق؛ فيمكن لتكنولوجيا الذكاء الاصطناعي والتعلم الآلي من تدعيم السياسة الجنائية المعاصرة للوقاية من الجرائم وخاصة جريمة التزييف العميق محل الدراسة من خلال التبصر المبكر بالسلوك الإجرامي ودقة الاستشعار به، وذلك من خلال تفسير علاماته الدالة عليه وتحليل المعلومات والبيانات بطريقة أكثر موثوقية، علاوة على ذلك؛ فإن الشركات التجارية الكبيرة تقوم بالاستعانة بتقنيات الذكاء الاصطناعي لإدارة المخاطر العالية وكشف عمليات الاحتيال والتزييف والتصدي لها من أجل منع الجرائم والتنبؤ بها لمواجهة الخطورة الإجرامية في المستقبل⁽¹⁾. وتطبيقاً على ذلك؛ فقد

1 - الأمم المتحدة، مؤتمر الأمم المتحدة الرابع عشر لمنع الجريمة والعدالة الجنائية، كيوتو - اليابان، والمنعقد في الفترة من 20 - 27 أبريل 2020، ص 16. وانظر: كذلك التقرير الصادر عن الأمم المتحدة في عام 2018 بشأن التهديدات المتعلقة بإساءة استخدام الذكاء الاصطناعي للأغراض الإجرامية وحدد منها ثلاث فئات رئيسة، الفئة الأولى: التهديدات المرتبطة بالأمن الرقمي، والفئة الثانية: التهديدات المرتبطة بالأمن المادي، والفئة الثالثة: والتي تتعلق بموضوع دراسة التهديدات المتعلقة بالأمن السياسي. مثال على ذلك، التزييف العميق من أجل نشر الأخبار الزائفة والمضللة للتأثير على الحملات الانتخابية وسلوك جمهور الناخبين، بما يؤدي إلى تقويض الحق في النقاش العام لأفراد المجتمع. انظر: ذلك في:

Miles Brundage and others, The malicious use of artificial intelligence: forecasting, prevention and mitigation, February 2018; INTERPOL innovation paper, Artificial intelligence, INTERPOL global complex for innovation, 2018, p.2.

استعانت شركات منصات وسائل التواصل الاجتماعي الإلكتروني بتقنيات الذكاء الاصطناعي والتعلم الآلي في منع المحتوى غير المشروع والأخبار الزائفة والشائعات وخاصة تلك الناتجة عن مقاطع الفيديو والصور المزيفة تزييفا عميقا بواسطة خوارزميات الذكاء الاصطناعي. وانطلاقا مما سبق؛ فقد سعى العلماء في مجال التقنيات التكنولوجية والذكاء الاصطناعي للتفرقة ما بين مقاطع الفيديو الأصلية والمقاطع التي تم تزييفها بواسطة التزييف العميق باستخدام الذكاء الاصطناعي؛ فتم الاستعانة بتقنية فوتوبليثيسموغرافي (Photo PPG) (plethysmography)؛ بحيث يتم من خلالها الكشف عن التغيرات في تدفق الدم في الجسم للتفرقة ما بين مقاطع الفيديو الأصلية والمصطنعة باستخدام التزييف العميق؛ حيث قامت شركة أنتل باستخدام نظام (Fake Catcher) لكشف التزييف في مقاطع الفيديو، وبالرغم من نجاح البرنامج في الكشف عن مقاطع الفيديو المزيفة إلا أن هذا النظام محل انتقاد باعتباره غير قادر على تحليل الصوت، وبناء على ذلك؛ فقد صنف هذا النظام بعد مقاطع الفيديو الحقيقية على أنها مزيفة من خلال الاستماع إلى الصوت؛ مما قد يتسبب في مشاكل على اعتبار المقطع في واقع الأمر أصلي وليس مزيفا⁽¹⁾. ونظرا لاستخدام تقنيات الذكاء الاصطناعي في التزييف العميق بحيث أصبح في الإمكان جعل المحتوى المزيف تزييفا عميقا أقرب إلى المحتوى الحقيقي بشكل يصعب فيه على الرجل المعتاد اكتشاف التزييف العميق، إلا أنه يمكننا وبواسطة تقنيات الذكاء الاصطناعي اكتشاف مقاطع الفيديو والصور المزيفة تزييفا عميقا من خلال ما يلي⁽²⁾ :

1 - في حالة وجود تغيير مفاجئ في الإضاءة الموجهة إلى الشخص في مقطع الفيديو بشكل غير طبيعي.

1 - أ. جيمس كلايتون، بي بي سي برنامجا للتدقيق في التزييف العميق في الأخبار، في 24 يوليو 2023، انظر: الموقع الإلكتروني:

<https://www.bbc.com/arabic/articles/c0xv408l61go>

تاريخ الزيارة 2024/8/27.

2 - انظر: دليل التزييف العميق، المرجع السابق، ص، 13.

2 - في حالة وجود تغيير بشكل غير طبيعي أو فوضوي في حركة وجه الشخص أو رمش العين بشكل متكرر أو عدم رمشها مطلقا، أو تغير لون البشرة في مقطع الفيديو.

3 - في حالة وجود تشوه بمنطقة الرقبة أو بالمنطقة التي تحيط بالوجه في مقطع الفيديو والصور.

4 - في حالة وجود عدم تطابق بين حركة الشفاه للشخص مع الكلام المسموع في مقطع الفيديو.

علاوة على ما سبق؛ فقد اعتمد موقع جوجل عبر جوجل للصور أداة داتا اكسيف (Exifdata) على تقديم خدمة مجانية يمكن للشخص معرفة ما إذا كان مقطع الفيديو أو صورة مبركة من عدمه، عبر نسخ الصور أو تحميل الرابط الخاص بمقطع الفيديو للتعرف على مصدقة المحتوى المرئي⁽¹⁾، كذلك خصصت منظمة العفو الدولية روابط يمكن من خلالها التحقق من مصداقية مقاطع الفيديو لمكافحة التضليل البصري الذي يعتمد على عرض محتوى مرئي مزيف تزييفا عميقا باستخدام خوارزميات الذكاء الاصطناعي سواء كان في شكل صور أم مقاطع فيديو مزيفة تزييفا عميقا.

ثانيا. آليات التعاون الدولي في مكافحة جريمة التزييف العميق باستخدام خوارزميات الذكاء الاصطناعي:

نظرا للطبيعة الخاصة لجرائم التزييف العميق باستخدام تقنيات الذكاء الاصطناعي باعتبارها من الجرائم الإلكترونية التي يتم ارتكابها عن بعد وبطريقة عابرة للحدود الوطنية؛ لذلك فقد شجع مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة عبر الوطنية الدول الأطراف في عام 2016 على ضرورة الاستفادة من التقنيات التكنولوجية من أجل

1 - د. لامية طالة، الصورة الإعلامية وإشكالية المصادقية في عصر الـ (Deep fake) قراءة في بعض الأمثلة العربية، المجلة الجزائرية للأمن الإنساني، المجلد 7، العدد الأول، الجزائر، يناير 2022، ص 206.

تسهيل التعاون بين الدول في مكافحة هذا النوع من الجرائم⁽¹⁾. وتطبيقا على ذلك، استخدام تقنيات التكنولوجيا الحديثة والتي تتيح استخدام المنصات الإلكترونية لإدارة طلبات التعاون الدولي للمساعدة القانونية المتبادلة سواء كانت في شكل صادر أم وارد أم تجميع كافة المعلومات والبيانات الإحصائية عن القضايا والاتجاهات وخاصة جريمة التزيف العميق⁽²⁾، وذلك على خلاف استخدام الأساليب التقليدية في إدارة طلبات المساعد القانونية من خلال السجلات الورقية؛ مما يوفر الوقت والجهد ويضمن سرعة إرسال واستلام المعلومات والبيانات خاصة في ظل استخدام الجناة للتقنيات التكنولوجية والذكاء الاصطناعي في ارتكاب جرائمهم، وخاصة جريمة التزيف العميق محل الدراسة.

ثالثا: الضمانات الإجرائية واحترام حقوق الإنسان في مكافحة جرائم التزيف العميق:

في واقع الأمر يجب توفير الضمانات الإجرائية واحترام حقوق الإنسان أثناء الإجراءات الجنائية في جريمة التزيف العميق باستخدام تقنيات الذكاء الاصطناعي، ويتمثل ذلك في تطبيق الضمانات الإجرائية المتعلقة بمدى قبول الأدلة المتحصلة بأساليب التحري والاستدلال أمام المحاكم الجنائية، بما في ذلك الأدلة التي تتطلب استخدام تقنيات التكنولوجيا وخوارزميات الذكاء الاصطناعي، ونستطيع أن نجمل هذه الضمانات على النحو التالي⁽³⁾:

1 - انظر: مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود الوطنية، قرار المؤتمر رقم 1/8 لسنة 2016. علاوة على ذلك، ففي عام 2018 تم تأسيس فريق من الخبراء الحكوميين الدوليين معني بإجراء دراسات شاملة عن الإشكاليات الناتجة عن الجرائم السيبرانية ومنها التعاون الدولي في هذا المجال، وذلك في الدورة السابعة والعشرين للجنة منع الجريمة والعدالة الجنائية، والتي انعقدت في مايو 2018، بالتعاون مع الفريق المعني بالتعاون الدولي لمؤتمر الأطراف اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود الوطنية.

2 - Asian development bank and organization for economic cooperation and development, Mutual legal, Assistance in Asia and the pacific: Experiences in 31 Jurisdictions, 2017, p. 31.

3 - Dimosthenis Chrysikos, Article 50: special investigative techniques, in the United Nations convention against corruption, a commentary, Cecily Rose, Michael kubiciel and Oliver Landwehr, eds., Oxford commentaries, on International Law Series, Oxford University press, 2019, p. 507.

- 1 - يتطلب جمع الأدلة في هذه الأنواع من الجرائم الالتزام الصارم بالضمانات لمواجهة إمكانية إساءة استخدام السلطة، بما في ذلك الإشراف القضائي على استخدام هذه السلطات لتقنيات وتكنولوجيا وخوارزميات أنظمة الذكاء الاصطناعي.
- 2 - ضرورة مراعاة مبادئ الشرعية الإجرائية الجنائية وحالة الضرورة والتناسب والموازنة بينها.
- 3 - ضرورة أن تمثل الأدلة الإلكترونية للإجراءات الجنائية المعمول بها حتى تكون مقبولة للإثبات أمام المحاكم الجنائية، بحيث يتم التحقق من مصداقية وفاعلية الدليل بواسطة الخبراء الفنيين في مجال تقنيات المعلومات والذكاء الاصطناعي.
- 4 - يتم مناقشة الأدلة التي تكون في شكل محتوى رقمي صوتي أو مرئي من قبل أطراف الدعوى الجنائية المنظورة أمام المحكمة بشكل علني في جلسات المحاكمة⁽¹⁾، بحيث يستطيع القاضي في النهاية من تكوين عقيدته بخصوص قيمة الدليل المستمد من المحتوى الرقمي الصوتي أو المرئي دون أي شك أو ظن في تزييفه أو اصطناعه عبر تقنيات الذكاء الاصطناعي والتعلم الآلي.

رابعاً. التدابير الوقائية والاحترازية لمواجهة التزييف العميق باستخدام تقنيات الذكاء الاصطناعي:

تتعدد التدابير الوقائية للحماية من التزييف العميق باستخدام خوارزميات الذكاء الاصطناعي، ويمكن لنا الاعتماد في هذا المجال على موقف المشرع الأوروبي بموجب اللائحة الأوروبية لخدمات الرقمية (DAS)⁽²⁾ والتي تشمل ما يلي:

1 - د. مصطفى صلاح عبد الحميد، التزييف الرقمي وأثره على حجية الأدلة الرقمية في الدعاوى الجنائية، دراسة فقهية مقارنة، مجلة الشريعة والقانون، العدد الأربعون، كلية الشريعة والقانون بالقاهرة، جامعة الأزهر، القاهرة، 2022، ص، 859، 858.

2 - Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), PE/30/2022/REV/1, 60 – 66.

- 1 - التحذير المسبق من قبل مقدمي خدمات المنصات الإلكترونية وأنظمة الذكاء الاصطناعي؛ حيث يجب على المنصات عبر الإنترنت إرسال تحذير مسبق قبل اتخاذ قرار التعليق المؤقت لممارسة الأنشطة عبر الإنترنت والمنصات الإلكترونية للشخص مرتكب السلوك غير المشروع؛ فينبغي أن يتضمن رسالة التحذير أسباب التعليق المحتمل للأنشطة عبر المنصة الإلكترونية، وكذلك حق الشخص المتلقي للرسالة التحذيرية في الطعن على هذه الرسالة كوسيلة من وسائل الانتصاف ضد قرار مقدمي المنصة عبر الإنترنت، عند اتخاذ قرار التعليق.
 - 2 - التعليق المؤقت عن ممارسة الأنشطة عبر الإنترنت والمنصات الإلكترونية وأنظمة الذكاء الاصطناعي؛ فيجب على مقدمي خدمات منصات وسائل التواصل الاجتماعي الإلكترونية وغيرها من المنصات عبر الإنترنت تعليق الأنشطة غير المشروعة ذات الصلة مؤقتاً للشخص مرتكب السلوك غير المشروع وخاصة التزييف العميق باستخدام أنظمة الذكاء الاصطناعي للمحتوى سواء كان في شكل محتوى مرئي أم صوتي، وفي نفس الوقت دون الإخلال بحق مقدمي خدمات المنصات عبر الإنترنت في وضع الشروط والقواعد الخاصة بهم في شكل تدابير أكثر في حالة المحتوى غير القانوني حسب درجة الخطورة الإجرامية للسلوك المرتكب مثال التزييف العميق الإباحي للأطفال.
 - 3 - التزام مقدمي المنصات عبر الإنترنت بضمان الشفافية، عبر التمكين من التدقيق في قرارات الإشراف على المحتوى لمقدمي المنصات عبر الإنترنت ومراقبة انتشار المحتوى غير القانوني عبر الإنترنت وخاصة المحتوى المزيف تزييفا عميقا، ومنها الاحتفاظ بقاعدة البيانات والمعلومات والنشر والتي تحتوي قرارات وبيانات أسباب مقدمي الخدمات عبر الإنترنت في إزالة أو تقييد توفر المعلومات والبيانات والوصول إليها.
- التزام مقدمي الخدمات عبر الإنترنت بالحفاظ على قاعدة بيانات ومعلومات محدثة بشكل مستمر، ومنها الالتزام بتقديم البيانات والمعلومات والقرارات وبيان الأسباب في شكل موحد دون تأخير لا مبرر له عندما يطلب منه من قبل السلطات القانونية وفقا للقواعد المنصوص عليها في القانون.

الخاتمة

نخلص في نهاية هذا البحث إلى أن التزييف العميق باستخدام أنظمة الذكاء الاصطناعي يقصد به استخدام تقنيات وخوارزميات الذكاء الاصطناعي التي تعتمد على المزج بين التعلم العميق والتزييف العميق من أجل تغيير الحقيقة في المحتوى الصوتي أو المرئي للشخص ونشره دون موافقته، وفي هذه الحالة نجد أن تقنية التزييف العميق باستخدام تقنيات الذكاء الاصطناعي تعتمد بشكل أساسي على الشبكات العصبية للذكاء الاصطناعي التي تقوم بتحليل ومعالجة مجموعة من البيانات والمعلومات الرقمية بطريقة آلية، من أجل تقليد تعبيرات وجه الشخص المعني المراد تزييف صوته وصورته وتصرفاته بدون موافقته.

وبناء على ذلك تظهر الحاجة إلى مواجهة الخطورة الإجرامية لظاهرة التزييف العميق باستخدام تقنيات الذكاء الاصطناعي على أمن واستقرار المجتمع؛ فمما لا شك فيه أن المعلومات والبيانات المزيفة تزييفا عميقا باستخدام خوارزميات الذكاء الاصطناعي لها تأثير خطير على أمن وسلام المجتمع واستقراره، وذلك عبر استخدامها في التهديد والتشهير الإلكتروني لسمعة الأشخاص خاصة الأشخاص السياسيين والمشهورين، كذلك أصبحت تشكل مادة أساسية لحروب الجيل الخامس من نشر الشائعات والبيانات والمعلومات المضللة التي يكون لها تأثير على الرأي العام والديمقراطية في الدول. وقد خلصنا في نهاية البحث إلى مجموعة من النتائج والتوصيات على النحو التالي:

أولا: النتائج:

1- أن عصر الذكاء الاصطناعي يستوجب من التشريعات الجنائية المعاصرة إعادة النظر في قيمة الأدلة الرقمية والذكية في الإثبات الجنائي؛ مما يستوجب من المشرع ضرورة التدخل لوضع الضوابط القانونية والتقنية للاعتماد على الأدلة الرقمية والذكية في الإثبات أمام المحاكم، وذلك ضمانا لسلامتها من أي تحريف أو تزييف عميق باستخدام تقنيات الذكاء الاصطناعي.

2 - انتهينا في هذا البحث إلى أهمية النص في التشريعات الوطنية على قواعد خاصة للمكافحة الجنائية لظاهرة التزييف العميق باستخدام أنظمة الذكاء الاصطناعي باعتبارها من الظواهر الإجرامية الحديثة سريعة الانتشار في العصر الرقمي والذكاء الاصطناعي من أجل مواكبة المتغيرات التكنولوجية الحديثة، وذلك من خلال اتباع سياسة تشريعية معاصرة وفعالة لمكافحة كافة الاستخدامات غير المشروعة لتقنية التزييف العميق باستخدام تقنيات الذكاء الاصطناعي على المدى الطويل، دون أي إعاقة لإمكانيات الاستخدام المشروع لهذه التقنية التكنولوجية الحديثة.

3 - كذلك توصلنا في هذه الدراسة إلى أهمية وضع مجموعة من الالتزامات على مزودي الخدمة والناشرين والمشغلين لأنظمة الذكاء الاصطناعي تضمن الشفافية للحماية من كافة صور التزييف العميق باستخدام الذكاء الاصطناعي، ومثال على ذلك، ما نص عليه المشرع الأوروبي في اللائحة الأوروبية بشأن الذكاء الاصطناعي رقم 1679 لسنة 2024 على التزام مشغلي تلك الأنظمة الذكية ومزودي الخدمات وناشريه بمجموعة من الالتزامات لضمان الشفافية، منها: تبصير المشاهد والمستخدم لهذه الأنظمة الذكية بأن الصور أو مقاطع الفيديو مزيفة تزييفا عميقا باستخدام تقنيات الذكاء الاصطناعي.

4 - إمكانية استخدام تقنيات التكنولوجيا الحديثة كفرصة لتطوير التعاون القانوني بين الدول، وذلك عبر استخدام المنصات الإلكترونية لإدارة طلبات التعاون الدولي للمساعدة القانونية المتبادلة سواء كانت في شكل صادر أم وارد أم تجميع كافة المعلومات والبيانات الإحصائية عن القضايا والاتجاهات وخاصة جريمة التزييف العميق.

ثانيا: التوصيات:

1 - ضرورة أن تستفيد أجهزة إنفاذ القانون والعدالة الجنائية بكافة أوجه التقدم في مجال تقنيات التكنولوجيا وخوارزميات أنظمة الذكاء الاصطناعي والتعلم الآلي من أجل مكافحة الظواهر

الإجرامية الجديدة والمعاصرة، مثل ظاهرة التزييف العميق باستخدام تقنيات الذكاء الاصطناعي؛ حيث إن مرتكبي هذا النوع من المجرمين يتميزون بالمعرفة والقدرة العالية على استخدام تقنيات التكنولوجيا وخوارزميات أنظمة الذكاء الاصطناعي؛ مما يتطلب من أجهزة إنفاذ القانون والعدالة الجنائية الاطلاع على هذه الأساليب الحديثة والمتقدمة من التكنولوجيا وخوارزميات الذكاء الاصطناعي من أجل مسايرة تطورات العصر الحديث، عصر المعرفة والذكاء الاصطناعي والتعلم العميق والروبوتات.

2 - ضرورة وضع قانون خاص لمكافحة ظاهرة التزييف العميق؛ خاصة تلك التي تتم باستخدام تقنيات الذكاء الاصطناعي وذلك على غرار ما نص عليه المشرع الأوروبي، لما تمثله هذه الظاهرة الإجرامية الحديثة من تهديد للقيم السائدة في المجتمع وكذلك نشر الأخبار الكاذبة والمضللة للإعلام ولجمهور المشاهدين، الأمر الذي يكون له تأثير خطير على الأمن والسلامة العامة في المجتمع وتهديد لاستقرار الدول؛ خاصة في ظل حروب الجيل الخامس والتي تعتمد على التضليل الإعلامي من خلال اصطناع ونشر المعلومات والبيانات الكاذبة عبر المحتوى المرئي والصوتي المفبرك بالتزييف العميق باستخدام خوارزميات الذكاء الاصطناعي بين أفراد المجتمع على منصات وسائل التواصل الاجتماعي الإلكتروني وتطبيقات التراسل الإلكترونية وغيرها من وسائل التواصل الإلكترونية الحديثة.

3 - ضرورة رفع كفاءة أجهزة إنفاذ القانون عن طريق بناء الخبرات والقدرات اللازمة لرجال الشرطة ووكلاء النيابة والقضاة؛ لمكافحة ظاهرة التزييف العميق باستخدام تقنيات الذكاء الاصطناعي، وذلك في جميع القطاعات ذات الصلة للسماح بالاستخدام الأمثل لتقنيات الذكاء الاصطناعي كفرصة لمكافحة هذه الظاهرة الإجرامية، وفي الوقت نفسه حماية حقوق ضحايا هذه الظاهرة الإجرامية.

4 - ضرورة أن تمثل الأدلة المستمدة من أنظمة الذكاء الاصطناعي للإجراءات الجنائية

المعمول بها حتى تكون مقبولة للإثبات أمام المحاكم الجنائية؛ بحيث يتم التحقق من مصداقية وفاعلية الدليل الذكي بواسطة الخبراء الفنيين في مجال تقنيات المعلومات والذكاء الاصطناعي.

5 - ضرورة أن تتخذ الشركات الكبيرة في مجال منصات وسائل التواصل الاجتماعي الإلكتروني كافة التدابير الاحترازية والوقائية لمكافحة المحتوى الصوتي والمرئي غير المشروع؛ خاصة مقاطع الفيديو والصور المزيفة تزييفا عميقا باستخدام تقنيات الذكاء الاصطناعي، من حيث إلزام مقدمي الخدمات الرقمية والمشغلين لأنظمة الذكاء الاصطناعي بالكشف والإبلاغ المبكر عنها، واتخاذ كافة السبل لإزالة ومحو هذا المحتوى غير المشروع من على المنصات الإلكترونية وإبلاغ الجهات القانونية المختصة لملاحقة مرتكبي هذا النوع من الجرائم لمكافحة إفلات الجناة من العقاب.

6 - نشر وتعزيز قيم الفهم للمخاطر التي يشكلها الاستخدام غير المشروع لتقنيات التكنولوجيا وخوارزميات الذكاء الاصطناعي والتعلم الآلي؛ بحيث يتم باستمرار رصد التطورات التكنولوجيات والتقنيات الحديثة لضمان مواجهتها ومعالجة المشاكل الناتجة عنها في ضوء الالتزام بالمساءلة والشفافية والنزاهة، وتطبيق المعايير الدولية والأخلاقية في استخدام تلك التكنولوجيات والتقنيات الحديثة بما يعزز ثقة الأفراد والمجتمع في استخدامها.

قائمة المراجع

أولا. قائمة المراجع باللغة العربية:

- أحمد الخولي، المسؤولية المدنية الناتجة عن الاستخدام غير المشروع لتطبيقات الذكاء الاصطناعي «الديب فيك نموذجاً»، مجلة البحوث الفقهية والقانونية، العدد 36، إصدار أكتوبر 2021.

- جواحي عبد الستار، جرائم الحاسوب، دراسة مقارنة بين الشريعة الإسلامية والقانون الجزائري، مذكرة تخرج لنيل شهادة الماجستير في العلوم الإسلامية، قسم العلوم الإنسانية، كلية العلوم الاجتماعية والإنسانية، جامعة الشهيد حمه لخضر، الجزائر، 2015، التمهيد.

- جيمس كلايتون، بي بي سي برنامجاً للتدقيق في التزييف العميق في الأخبار، في 24 يوليو 2023، انظر الموقع الإلكتروني:

<https://www.bbc.com/arabic/articles/c0xv408l61go>

تاريخ الزيارة 27/8/2024.

- لامية طالة، الصورة الإعلامية وإشكالية المصادقية في عصر الـ (Deep fake) قراءة في بعض الأمثلة العربية، المجلة الجزائرية للأمن الإنساني، المجلد 7، العدد الأول، الجزائر، يناير 2022.

- ليليا بوسحرة، د. عبد القادر بودربالة، التزييف العميق والدعاية الرقمية في عصر التمكين الرقمي: قراءة في النماذج والرهانات، مجلة مصداقية، المدرسة العليا العسكرية للإعلام والاتصال، مجلد 5، عدد 1، الجزائر، 2023.

- مارتن أندرسون، مقترحات تنظيم التزييف العميق لأوروبا والمملكة المتحدة، في 9 ديسمبر 2022، الموقع الإلكتروني:

- <https://www.unite.ai/ar/european-and-uk-deepfake-regulation-proposals-are-surprisingly-limited/>

تاريخ الزيارة 30 أغسطس 2024.

- ماري شروتير، الذكاء الاصطناعي ومكافحة التطرف العنيف، تقرير في منشورات الشبكة العالمية لمكافحة التطرف التكنولوجي GNET، ص 17، على الموقع الإلكتروني:

www.gent-research.org

تاريخ الزيارة 2 سبتمبر 2024.

- مصطفى عبد الحميد، التزييف الرقمي وأثره على حجية الأدلة الرقمية في الدعاوى الجنائية، دراسة فقهية مقارنة، مجلة الشريعة والقانون، العدد الأربعون، كلية الشريعة والقانون بالقاهرة، جامعة الأزهر، القاهرة، 2022.

- معين الميتمي، التزييف العميق، مستقبل القوانين المنظمة للبرمجيات الذكية، وذلك على الموقع الإلكتروني:

<http://al-ain.com/article/deepfake-the-futue-of-smart-software-law>.

تاريخ الزيارة 2 سبتمبر 2024.

ثانيا : قائمة المراجع باللغة الأجنبية:

- Ajder H., Patrini G., at, The state of deepfakes: landscape, threats, and impact, Amsterdam, 2019, Deepttrace, site V. 30/08/2024:

<http://regmedia.co.uk/2019/10/08/deepfake-report.pdf>.

- C. Neu Berghoff & A. Von Twickel, The interplay of AI and biometrics: challenges and opportunities, Computer, 54 (09), 2021.

- Cécile Crichton, Projet de règlement sur l'IA (II): une approche fondée sur les risques, Dalloz actualité 04 mai 2021, Sit:

[Diakopoulos Nicholas, Johnson Deborah, Anticipating and addressing the ethical implications of deepfakes in the context of elections, New media & Society, 2021, Vol, 23, \(7\).](https://www.dalloz.fr/documentation/Document?ctxt=0_YSR0MD1EZVWwIEZha2XCp3gkc2Y9c2ItcGxLXNIYXJjaA%3D%3D&ctxtl=0_cyRwYWdlTnVtPTHCP3MkdHJpZGF0ZT1GYWxzZcKncyRzb3J0PSNkZWZhdWx0X0Rlc2PCp3Mkc2xOYIBhZz0yMMKncyRpc2Fibz1UcnVlwqdzJHBhZ2luZz1UcnVlwqdzJG9uZ2xldD3Cp3MkZnJlZXNjb3BIPUZhbHNlwqdzJHdvSVM9RmFsc2XCp3Mkd29TUENI. V., Le 5 Avril 2024.</p>
</div>
<div data-bbox=)

- Dimosthenis Chrysikos, Article 50: special investigative techniques, in the United Nations convention against corruption, a commentary, Cecily Rose, Michael kubiciel and Oliver Landwehr, eds., Oxford commentaries, on International Law Series, Oxford University press, 2019.
- J. Wojewidka, The deepfake threat to face biometrics, Biometric Technology today, (2), 2020.
- Julie Groffe – Charrier, Vers un encadrement légal des deepfakes, le 12 juillet 2023, Dalloz Actualité, site:
https://www.dalloz-actualite.fr/flash/vers-un-encadrement-legal-des-deepfakes#results_box, V., Le 11 Sept 2023.

- K. M. Sayler & L. A. Harris, Deep fakes and national security, Congressional research SVC Washington, USA, 2020.
- L. Laishram, M. M. Rahman & S. K. Jung, Challenges and applications of face deepfake, In international workshop on frontiers of computer vision, Springer, Cham, February, 2021.
- Maras, Marie Helen, Alexandrou Alex, Determining authenticity of video evidence in the age of artificial intelligence and in the wake of deepfake videos, the international journal of evidence & proof, 2019, Vol, 23 (3).
- Miles Brundage and others, The malicious use of artificial intelligence: forecasting, prevention and mitigation, February 2018; INTERPOL innovation paper, Artificial intelligence, INTERPOL global complex for innovation, 2018, p.2.
- P. Li Q. Dong & J. Zheng, Enhancing the security of pattern unlock with surface EMG – based biometrics, Applied Sciences, 10 (2), 2020.
- S. G. Tesfagergish, R. Damasevicius & J. KAPOCIUTE - Dzikien, Deep fake recognition in tweets using text augmentation, Word embeddings and deep learning, In International conference on computational science and its applications, September, 2021.
- Wang S., Kim S., User's emotional and behavioral responses to deepfake videos of k-pop idols, computers in human behavior, site V. 30/08/2023:
<https://doi-org/10.1016/J.chb.2022.107305>.

- Wilkerson, Lindsey, The rising concerns of deepfake technology and its influence on democracy and the first amendment, Missouri Law, Review, 2021, Vol, 86, (1).
- Asian development bank and organization for economic cooperation and development, Mutual legal, Assistance in Asia and the Pacific: Experiences in 31 Jurisdictions, 2017.
- Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), PE/30/2022/REV/1, 60 – 66.
- Sénat, Projet de loi, Sécuriser et réguler l'espace numérique, (1) ère lecture, PROCÉDURE ACCÉLÉRÉE, n° 778 , 777, 3 juillet 2023, Site: https://www.senat.fr/amendements/2022-2023/778/Amdt_127.html, V., 11 sept 2024.
- Tribunal correctionnel de Versailles - 8e ch. Correctionnelle, 8e ch., 14 avril 2021 / n° 20167000022, Site: https://www.dalloz.fr/documentation/Document?id=TCORR_VERSAILLES_2021-0414_20167000022&ctxt=0_YSR0MD1EZWWwRmFrZcKneCRzZj1zaW1wbGUtc2VhcmNo&ctxtl=0_cyRwYWdlTnVtPTHCP3MkdHJpZGF0ZT1GYWxzZcKncyRzb3J0PSNkZWZhdWx0X0Rlc2PCp3Mkc2xOYlBhZz0yMMKncyRpc2Fibz1UcnVlwqdzJHBhZ2luZz1UcnVlwqdzJG9uZ2xldD3CP3MkZnJlZXNjb3BIPUZhbHNlwqdzJHdvSVM9RmFsc2XCp3Mkd29TUENIPUZhbHNlwqdzJGZsb3dNb2RIPUZhbHNlwqdzJGJxPcKncyRzZWYyZ2hMYWJlbD3CP3Mkc2VhcmNoQ2xhc3M9#texte-integral, V., Le 4 avril 2024.

ثالثاً: التقارير والأحكام القضائية:

- أوراق عمل مؤتمر الأطراف في اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود الوطنية، قرار المؤتمر رقم 8/1 لسنة 2016. علاوة على ذلك في عام 2018 تم تأسيس فريق من الخبراء الحكوميين الدوليين معني بإجراء دراسات شاملة، الإشكاليات الناتجة عن الجرائم السيبرانية ومنها التعاون الدولي في هذا المجال، وذلك في الدورة السابعة والعشرين لجنة منع الجريمة والعدالة الجنائية، والتي انعقدت في مايو 2018، بالتعاون مع الفريق المعني بالتعاون الدولي لمؤتمر الأطراف اتفاقية الأمم المتحدة لمكافحة الجريمة المنظمة العابرة للحدود الوطنية.

- أوراق عمل مؤتمر الأمم المتحدة الرابع عشر لمنع الجريمة والعدالة الجنائية، كيوتو - اليابان، والمنعقد في الفترة من 20 - 27 أبريل 2020.

- تقرير الأمم المتحدة في عام 2018 بشأن التهديدات المتعلقة بإساءة استخدام الذكاء الاصطناعي للأغراض الإجرامية، وحدد منها ثلاث فئات رئيسة، الفئة الأولى: التهديدات المرتبطة بالأمن الرقمي، والفئة الثانية: التهديدات المرتبطة بالأمن المادي، والفئة الثالثة: والتي تتعلق بموضوع الدراسة التهديدات المتعلقة بالأمن السياسي مثال على ذلك، التزييف العميق من أجل نشر الأخبار الزائفة والمضللة للتأثير على الحملات الانتخابية وسلوك جمهور الناخبين؛ بما يؤدي إلى تقويض الحق في النقاش العام لأفراد المجتمع.

- تقرير اللجنة الرقمية والثقافية والإعلام والرياضة، البرلمان البريطاني، مشروع قانون الأمان على الإنترنت، عام 2021.

- تقرير معهد الأمم المتحدة لبحوث نزع السلاح (UNIDIR) بشأن تداعيات الابتكارات التكنولوجية للذكاء الاصطناعي على الخصوصية الرقمية والأمن والثقة، خاصة ظاهرة التزييف العميق والثقة والأمن الدولي، في 25 أغسطس 2021، جنيف. انظر الموقع الإلكتروني:

<https://documents-dds-ny.un.org/doc/unidir.innvations-dialogue.com>

تاريخ زيارة الموقع الإلكتروني 31 أغسطس 2024.

- دليل التزييف العميق، البرنامج الوطني للذكاء الاصطناعي، دولة الإمارات العربية المتحدة، يوليو 2021.

- محكمة التمييز القطرية، تمييز جنائي، جلسة 16 أكتوبر 2017، الطعن رقم 63 لسنة 2017.

- محكمة التمييز القطرية، تمييز جنائي، جلسة 21 ديسمبر 2020، الطعن رقم 163 لسنة 2020.

- محكمة التمييز القطرية، تمييز جنائي، جلسة 3 فبراير 2020، الطعن رقم 139 لسنة 2020.

- محكمة النقض المصرية، نقض جنائي، جلسة 18 أكتوبر 1965، الطعن رقم 34 ق السنة 16.

- محكمة النقض المصرية، نقض جنائي، جلسة 8 ديسمبر 1964، الطعن رقم 331 سنة 34 ق،

السنة 15، ص 795. وكذلك نقض جنائي جلسة 28 يونيو 1965 طعن رقم 144 سنة 35 ق،

السنة 16، ص 361. وكذلك نقض جنائي، جلسة 4 أبريل 1976، الطعن رقم 1526 لسنة 45

ق، السنة 27.