مجلة جامعة الشارقة للعلوم القانونية

جامعة الشارقة
UNIVERSITY OF SHARJAH

مجلة جامعة الشارقة للعلوم القانونية

مجلة علمية محكمة

المجلد 22، العدد 1
رمضان 1446هـ / مارس 2025م

الترقيم الدولي المعياري للدوريات 2616-6526

https//:doi.org/10.36394/jls.v22.i1.12

المواجهة الجنائية للتلاعب بالمحتوى الرقمي باستخدام تقنيات التوليف العميق في التشريع الصيني
دراسة وصفية مقارنة

معاذ سليمان الملا[1]

تاريخ الاستلام: 03-12-2023 **تاريخ القبول: 19-04-2024**

ملخص البحث:

تطورت في الآونة الأخيرة أساليب التلاعب في المحتوى الرقمي عبر تطبيقات أطلق عليها المنظم الصيني مصطلح التوليف العميق (Deep Synthesis) وذلك بفضل تكنولوجيا الذكاء الاصطناعي التي حسنت من جودة المحتوى. وتتجلى أهمية البحث بأنه يناقش موضوعاً حديثاً نسبياً ظهر بسبب سوء استخدام هذه التطبيقات، فالمشكلة تتجسد في توظيف تلك التقنيات لتحقيق مقاصد غير مشروعة حتى ظهر لنا مصطلح جديد التزييف العميق (Deepfake) الذي يعبر عن إمكانية العبث بالمحتوى الرقمي بشكل يتقارب فيه مع المحتوى الحقيقي، فضلاً عن فقدان الضوابط الأخلاقية في إنتاج وتطوير هذه التقنيات بشكل سريع جداً. ونهدف في هذا البحث إلى بيان ماهية التلاعب بالمحتوى الرقمي باستخدام تقنيات التوليف العميق وتطبيقاتها، وواقع خطورة سوء استخدام (التزييف العميق) على أمن المجتمعات في البيئة السيبرانية ومدى اعتبار هذا التلاعب جريمة جنائية تخضع لمفهوم الجرائم السيبرانية، وكيف واجهت الصين باعتبارها من أوائل الدول التي وضعت لائحة للحد من مخاطر سوء استخدام هذه التقنيات والعقوبات المقررة لها وموقف القوانين الجنائية المقارنة. ومن أجل ذلك اعتمدنا في عرض البحث على المنهجين الوصفي والمقارن لبلوغ الهدف من البحث. لننتهي بعرض النتائج والتوصيات التي تضمن مواجهة فعالة لسوء استخدام تطبيقات التوليف العميق.

الكلمات الدالة: التوليف العميق، التزييف العميق، سوء الاستخدام، جريمة سيبرانية، الذكاء الاصطناعي، القانون الجنائي، المنظم الصيني

(1) كلية القانون الكويتية العالمية (الكويت – الكويت)

m.almulla@kilaw.edu.kw

المقدمة:

نجحت الثورة الصناعية الرابعة نجاحاً باهراً في إحداث نقلة نوعية في عمل الأنظمة الإلكترونية المختلفة، فقد نقلتها من مجرد أدوات تؤدي أعمالاً مؤتمتة ومحددة يتم برمجتها من قبل الإنسان إلى أنظمة ذكية تحاكي عقله وأنماطه السلوكية المختلفة بفضل تكنولوجيا الذكاء الاصطناعي وخوارزمياتها التي تتغذى على البيانات الضخمة لتتعلم الآلة وتتدرب على القيام بها دون أي تدخل من صانعها (Kaplan, 2016; Nilsson, 2009; الموسوي, 2019; هارون, 2019) ، فالمعادلة في البيئة السيبرانية أنه كلما زاد حجم البيانات التي يحصل عليها التطبيق من المستخدمين تحسّن الأداء وزادت جودة المحتوى وأصبح الناتج أقرب إلى الواقع

والذكاء الاصطناعي هو تكنولوجيا تعتمد على الخصائص الحاسوبية بحيث تمكن الآلة من محاكاة القدرات الذهنية البشرية وأنماط عملها بفضل ما تعالجه من بيانات، من بينها القدرة على التعلم والاستنتاج ورد فعل على أوضاع لم تبرمج في الآلة. لذلك عرف الذكاء الاصطناعي بتعريفات عديدة تنصب على قدرة الآلة على التعلم والاستقلالية في الأداء.

وتتجلى أهمية البحث في كونه يناقش موضوعاً حديثاً يتعلق في أساليب تمكن مستخدمي الهواتف المحمولة أو الحواسيب وغيرها من التلاعب بالمحتوى الرقمي على النحو الذي تتغير فيه الحقيقة عبر تقنيات أطلق عليها في الصين مصطلح التوليف العميق (Deep Synthesis) وقد تعددت تطبيقات هذه التقنيات في مجالات عديدة فمن خلالها يستطيع المستخدمون إنشاء محتوى رقمي أو تغييره كالصور والنصوص والمقاطع الصوتية أقرب إلى الحقيقة. وقد استفاد الكثيرون منها في العديد من المجالات كإنتاج الأفلام السينمائية وأيضاً في الدعاية والإعلان وفي الإعلام والصحافة وفي تطبيقات التسلية.

وتكمن المشكلة التي نطرحها بأن البعض وظف هذه التقنيات في تحقيق مقاصد غير مشروعة تؤثر على مفهوم الحقيقة وما يشكله ذلك– بطبيعة الحال- من خطر يهدد حقوق ومصالح الأفراد والدول على حد سواء لا سيما مع استخدام خوارزميات الذكاء الاصطناعي في إنتاج المحتوى الرقمي وفقدان الضوابط الأخلاقية والالتزامات في تطوير تلك التقنيات مما أظهر لنا مصطلح التزييف العميق

ومن هذا المنطلق طرحنا عدة أسئلة تضعنا الإجابة عنها أمام الأهداف التي نصبو إليها من إعداد هذا البحث، وهذه الأسئلة نوردها على النحو الآتي:

1. ما المقصود بتقنية التوليف العميق؟ وكيف تعمل هذه التقنية؟ وما مجالاته؟

2. كيف نقدر خطورتها؟ وما الطبيعة القانونية لسوء استخدامها؟

3. هل تقييد استخدام هذه التقنيات يشكل مساساً للحرية في البيئة السيبرانية؟

4. ما علاقة سوء استخدام هذه التقنية بالجرائم السيبرانية؟

5. ما موقف القوانين الجنائية من سوء استخدام تقنية التوليف العميق؟ وكيف تعاملت الصين معها؟

لقد ارتأينا أن المنهجين الوصفي والمقارن يلبيان متطلبات إعداد البحث، فالمنهج الوصفي استخدمناه من أجل وصف التلاعب بالمحتوى الرقمي باستخدام تقنيات التوليف العميق والطبيعة القانونية لسوء استخدام هذه التقنيات بعد تقدير خطورتها ومدى اعتبارها من قبيل الجرائم السيبرانية، واستخدمنا المنهج المقارن؛ إذ بينا موقف بعض القوانين المقارنة التي تناولت تجريم هذه الأنشطة مع مسلك الصين التي بادرت إلى وضع حلول تحد من سوء استخدام هذه التقنيات وصولاً إلى النتائج والتوصيات. وقد قمنا بتقسيم خطة البحث إلى ثلاث مطالب على النحو الآتي:

المبحث التمهيدي: ماهية التلاعب بالمحتوى الرقمي باستخدام تقنية التوليف العميق.

المبحث الأول: سوء استخدام تقنية التوليف العميق (التزييف العميق) المخاطر والطبيعة القانونية

المبحث الثاني: موقف القوانين الجنائية المقارنة من أفعال التزييف العميق

المبحث الثالث: موقف الصين من سوء استخدام تقنية التوليف العميق.

المبحث التمهيدي: ماهية التلاعب بالمحتوى الرقمي باستخدام تقنية التوليف العميق

إن مفهوم المحتوى الرقمي مفهوم واضح وجلي، فمن منا لا يعرف هذا المحتوى الذي فرضه الواقع التكنولوجي في العديد من التعاملات، فهذا المفهوم ينصرف إلى مجموعة البيانات والمعلومات التي يتم احتواؤها ومعالجتها في الأنظمة التكنولوجية المختلفة كالحاسب الآلي والهاتف النقال وغير ذلك من أدوات يستخدمها الشخص الطبيعي والاعتباري في تعاملاتهما عبر هذه الأنظمة.

المطلب الأول: المقصود بالتلاعب بالمحتوى الرقمي:

نقصد بالتلاعب بالمحتوى الرقمي القيام بتغيير المحتوى(فبركة) أي خلق واقع مشابه للحقيقة عن طريق برامج إلكترونية أو ذكية من شأنها أن تضلل الأشخاص عن حقيقة موضوع معين أو تثير الشكوك حوله، وقد أتاحت هذه التقنية للآخرين استخدام أدواتها دون وضع ضوابط فنية لهذا الاستخدام مما أدى إلى إرباك المتابعين بحقيقة الموضوعات المتداولة في البيئة السيبرانية.

وقد أطلق المنظم الصيني مصطلح التوليف العميق وباللغة الإنجليزية (Deep Synthesis)- للتعبير عن التلاعب في المحتوى الرقمي، وذلك على خلاف المصطلح الذي استخدمه البعض؛ إذ اشتهرت بمصطلح التزييف العميق وباللغة الإنجليزية (Deepfake). وسوف نشير لاحقاً إلى الفرق بينهما.

وقد ظهرت هذه التقنية منذ سبعينات القرن الماضي في معالجة المحتوى الرقمي حتى القرن العشرين الذي شهد تعاظماً ملفتاً في تطوير هذه التقنية باستخدام الذكاء الاصطناعي؛ إذ اعتمدت على التعلم العميق والتعلم الآلي (فاضل & عباس, 2022)، ويذكر أن هذا التطبيق بدت ملامح ظهوره عام 1997عبر برنامج Video Rewrite الذي يعالج الصور والمقاطع الرقمية (Bregler et al., 2023) على نحو مزيف، وقد شهد هذه التقنية تطوراً حتى ظهر مصطلح التزييف العميق عام 2017 بعدما تم استخدامها في تبديل وجه أحد المشاهير بوجه ممثل إباحي، وفي عام 2018 أصبح التطبيق في متناول الجميع بشكل مجاني عبر شبكة الإنترنت (Gerstner, 2020; Nguyen et al., 2022; إبراهيم, 2021) .

وأصبحت هذه التقنية- بفضل الثورة الصناعية الرابعة-مدعمة بخوارزميات الذكاء الاصطناعي أي أن تزييف المحتوى سوف يكون في واقع الأمر أكثر دقة بحيث يصعب التمييز بين المحتوى الأصلي والمحتوى غير الأصلي (Sloot et al., 2021) . وقد عرفها البعض بأنها التقنية التي يتم من خلالها تصنيع الوسائط المتعددة المختلفة سواء كانت فيديوهات أو أصواتاً أو صوراً مزيفة من خلال برامج الحاسوب المبرمجة بتقنيات الذكاء الاصطناعي. أو هي تقنية تستخدم الذكاء الاصطناعي لتزييف الصور، أو الفيديو، أو الصوت بدمجها، أو استبدالها، أو تركيبها لجعلها تبدو أصلية (Westerlund, 2019). وعرفها قانون ولاية تكساس الأمريكية بأنها" مقطع فيديو تم إنشاؤه باستخدام الذكاء الاصطناعي، والذي يبدو، بقصد الخداع، أنه يصور شخصًا حقيقيًا يقوم بعمل لم يحدث في الواقع".

ويختلف الوضع بالنسبة للائحة الصينية الخاصة بتنظيم أحكام التوليف العميق النافذة بتاريخ 10 يناير2023 (Chinese Congress, 2020)، وقد عرفت هذه التقنية في المادة

23 منهـا بأنهـا "اسـتخدام تقنيـات مثـل التعلـم العميـق والواقـع الافتراضـي، التـي تسـتخدم خوارزميـات التسلسـل التوليـدي لإنشـاء نـص أو صـور أو صـوت أو فيديـو أو مشـاهد افتراضيـة أو معلومـات أخـرى..".

المطلب الثاني: آلية عمل تقنية التوليف العميق وأهم مجالاتها:

إن آليـة عمـل تقنيـة التوليـف العميـق لـم تكـن حديثـة، بـل موجـودة منـذ فتـرة زمنيـة فقـد تعاملـت المحاكـم الأمريكيـة مـع القضايـا المتصلـة بعمليـات التزويـر والتلاعـب فـي المحتـوى الرقمـي عبـر الحاسـب الآلـي، فمنذ ظهـور برنامـج Adobe Photoshop يسـتطيع المسـتخدمون التلاعـب بالصـور(Reynolds, 2020)

تعتمـد آليـة عمـل تقنيـة التوليـف العميـق علـى المحتـوى الرقمـي الـذي يصفـه البعـض بوقـود الثـورة الصناعيـة الرابعـة أو الغـذاء لهـا (Tyagi, 2023; عبـد الصـادق, 2018) أو تعـد آليـة عمـل هـذه التقنيـة معقـدة جـداً؛ إذ يسـتخدم التطبيـق مجموعتيـن منفصلتيـن مـن الخوارزميـات تعـملان معًـا: الخوارزميـة الأولـى يُطلـق عليهـا المولـدة (Generator) وتعمـل علـى إنتـاج محتـوى مزيـف، بينمـا الثانيـة هـي خوارزميـةُ يطلـق عليهـا مميـزة (Discriminator) لأنهـا تحـاول تحديـد مـا إذا كان الفيديـو حقيقيًـا أم مزيفـاً؟ فكلاهمـا يتنافسـان فـإذا تمكنـت الخوارزميـة الثانيـة مـن معرفـة أن الفيديـو مزيـف، فـإن الخوارزميـة الأولـى تحـاول مـرة أخـرى؛ إذ تسـتمر المنافسـة حتـى تقـوم الشـبكة الأولـى بإنتـاج محتـوى تُصنفـه الشـبكة الثانيـة بأنـه حقيقـي وتعـرف بالشـبكات التوليديـة التنافسـية (GANs). ويمكـن الاعتمـاد علـى تقنيـة أخـرى باسـتخدام الـذكاء الاصطناعـي مـن خلال أداة الترميـز التلقائـي (Autoencoder).

تُسـتخدم هـذه الأداة عـادةً فـي تقنيـة تبديـل أو اسـتبدال الوجـوه فـي الصـور ومقاطـع الفيديـو. وذلـك عـن طريـق تدريـب أداة الترميـز باسـتخدام آلاف الصـور التـي تتضمـن لقطـات الوجـه للشـخصين المسـتهدفين بالتقنيـة. فتقـوم تلـك الأداة باسـتخراج الميـزات الأساسـية وإيجـاد أوجـه التشـابه بيـن تلـك الصـور. ثـم بعـد ذلـك تقـوم أداة فـك الترميـز بإعـادة بنـاء الصـور واسـتبدال الوجـوه (Westerlund, 2019; Yasrab et al., 2021; فاضـل & عبـاس, 2022; محـرم, 2022).

ومـن أمثلـة أنظمـة التلاعـب المعروفـة برنامـج أدوبـي لمعالجـة اللغـات الطبيعيـة VoCo فمـن خلالـه يمكـن تقليـد الأصـوات بدقـة، كذلـك أنظمـة التعـرف علـى الصـورELMO التـي تتعلـم قـراءة لصقـات البيانـات الفوضويـة، وسـوف تصبـح قـادرة علـى التأليـف. وكذلـك برنامـج Face2Face الـذي يمكـن مـن خلالـه التلاعـب بالوجـوه فـي الفيديوهـات والصـور وإلـى غيـر ذلـك مـن إمكانـات، ولا نعلـم مـاذا يخفـي لنـا المسـتقبل القـادم مـن إمكانيـات تعـدم الحقيقـة قـد عبـر

عنها البعض كما سوف نرى مع تطوير إمكانياتها عبر الذكاء الاصطناعي(Coleman, 2020; فاضل & عباس, 2022).

وقد أوردت المادة 23 من اللائحة -المشار إليها سابقاً - نماذج أو أنماطاً جاءت على سبيل المثال وليس الحصر لحالات التوليف العميق تضعنا أمام توسع اللائحة في تحديد مفهوم هذه التقنية حيث شملت كافة أشكال التلاعب بالمحتوى الرقمي وقد نصت اللائحة على ما يلي:

1. تقنيات إنشاء محتوى نصي أو تحريره، مثل إنشاء الفصل وتحويل نمط النص وحوارات الأسئلة والأجوبة.
2. تقنيات إنشاء محتوى صوتي أو تحريره، مثل تحويل النص إلى محادثة وتحويل الصوت وتحرير سماته.
3. تقنيات إنشاء محتوى غير صوتي أو تحريره، مثل الموسيقى وتحرير صوت المشهد.
4. تقنيات إنشاء أو تحرير السمات البيوميترية مثل الوجوه في الصور ومحتوى الفيديو، مثل إنشاء وجه أو تبديله أو تحرير السمات الشخصية أو التلاعب بالوجه أو التلاعب بالإيماءات.
5. تقنيات تحرير السمات غير البيوميترية في الصور ومحتوى الفيديو، مثل تحسين الصورة واستعادتها.
6. تقنيات إنشاء أو تحرير المشاهد الافتراضية مثل إعادة البناء ثلاثي الأبعاد.

ومن خلال هذه التعريفات نجد أن المنظم الصيني قد شمل بمفهومه كافة الأشكال التي يمكن أن تظهر بالمستقبل عبر تطبيقات إلكترونية تمكن المستخدمين من تغيير مضمونها الحقيقي سواء كان بالتلاعب في الصوت أو الصورة أو المقاطع.

وفيما يتعلق بتطبيقاتها فالواقع يكشف عن استخدام هذه التقنية في العديد من المجالات مثل مجال الطب والرعاية الصحية ويمكن توظيف هذه التقنية لخدمة المرضى الذين فقدوا أصواتهم، أو استخدامها في إخفاء هويتهم (Shin et al., 2018). ويمكن استخدامها في مجال الترفيه والتسلية وعقد اللقاءات فقد أصبح البعض يستفيد من هذه التقنية من خلال تغيير الوجوه أو الصور في الألعاب الإلكترونية وحتى في اللقاءات واجتماعات العمل وغيرها(Caporusso, 2021; Ghaemmaghami & Villafranco, 2021)، وقد أصبحت هذه التقنية مطبقة في بيئة الميتافيرس(Tariq et al., 2023) (Metaverse) .

وفي مجال الإنتاج الفني والسينمائي يمكن الاستفادة منها في تصوير المقاطع الخيالية، بل يمكن إحياء المتوفين من خلال استخدام صورته(Lexology, 2021) ، وتعد الكلفة المالية لهذه التقنية في هذا المجال قليلة كونها تعتمد على برامج حاسوبية مجهزة لهذه الأغراض. وفي مجال الأنشطة التجارية يمكن استفادة العلامات التجارية منها في الدعاية والإعلان عن المنتجات كتركيب أوجه المشاهير في الدعاية للتأثير في الجمهور وزيادة الإقبال على المنتجات المختلفة، وقد استخدم هذا الأسلوب كثيراً في أثناء جائحة كورونا (Ghaemmaghami & Villafranco, 2021)

المبحث الأول: سوء استخدام تقنية التوليف العميق (التزييف العميق): المخاطر والطبيعة القانونية

على الرغم من الاستفادة العملية لاستخدام تقنية التوليف العميق، إلا أنه بالمقابل يكشف سوء استخدامها عن خطورة بالغة على مفهوم الحقيقة لاسيما بعد تطوير إمكانياتها عبر خوارزميات الذكاء الاصطناعي. ومن هذا المنطلق نحاول أن نقدر خطورة سوء استخدام هذه التقنية حتى يتسنى لنا تحديد طبيعتها القانونية.

المطلب الأول: خطورة إساءة استخدام هذه التقنية على مفهوم الحقيقة:

قد عبر البعض عن خطورة إساءة استخدام هذه التقنية على مفهوم الحقيقة بالقول بأن" التزييف العميق هو المكان الذي تموت فيه الحقيقة.. إذ يمكن للتكنولوجيا أن تجعل الأمر يبدو كما لو كان الشخص قال أو فعل أي شيء" (Schwartz, 2018). كما أشار مركز الأمن القومي الأمريكي إلى أن" الاستخدام الكبير للأخبار الزائفة يمكن أن يسبب نهاية الحقيقة في نهاية المطاف" (Horowitz et al., 2018). كذلك عبرت محكمة الاستئناف في كولورادو الأمريكية عن الخطورة مصداقية الأدلة المستمدة في الجرائم المرتبطة بتكنولوجيا الحاسوب وإمكانية تغييرها بقولها "أن التطورات في تكنولوجيا الحاسوب تمكن تقريبًا أي مالك لجهاز شخصي المعرفة اللازمة من تحرير التسجيلات بشكل زائف ... لكن الحقيقة أن التزوير في التسجيلات الإلكترونية أمر ممكن دائمًا.." (Colorado Court of Appeals, 2019). وهذه العبارات توضح أن واقع انتشار محتوى رقمي قريب للحقيقة أو بمعنى آخر محتوى غير حقيقي تم التلاعب به باستخدام تقنيات التوليف العميق أو محتوى مزيف إنما يشكل خطراً يهدد حقوق ومصالح الآخرين وقد واجهت الصين هذه الأنشطة من خلال تنظيم لائحة خاصة لاستخدام هذه التقنيات وحددت المسؤولية عن الإخلال بأحكامها(Sheehan, 2023) .

فجوهر خطورة سوء استخدام تقنية التوليف العميق يتمثل في تغيير الحقائق على خلاف الواقع، فأصبح من السهل توجيه الرأي العام وتضليله من خلال استغلال هذه التقنية بنشر أخبار زائفة تضلل الجمهور (Langa, 2021) . وأشهر مثال يمكن الاستدلال به هو التدخل في سير الانتخابات الأمريكية عام 2016 حيث صدق عدد كبير من الناس أمراً خاطئاً وهو تأييد الفاتيكان لدونالد ترامب (Coleman, 2020) ، كذلك مقطع مفبرك للرئيس السابق دونالد ترامب يظهر وعده برفع الرسوم الجمركية على واردات الصلب، وقد أثر ذلك سلباً على أسعار أسهم الشركة في البورصة (AI-Business, 2019) . ويمكن استخدامها في الإساءة والإضرار بالغير: ويمكن للمسيئين استغلال المحتوى الرقمي المنشور على شبكة الإنترنت أو على الحسابات الشخصية للأفراد سواء بموافقهم أو بدونها (Delfino, 2019) ، من خلال تركيب صور أو أصوات أو مقاطع للسخرية أو الانتقام أو صناعة مواد إباحية أو غير ذلك ترفع من مستويات التنمر أو الابتزاز الإلكتروني ضدهم أو يضع الغير موضع احتقار المجتمع (فاضل & عباس, 2022; محرم, 2022).

فالذي يجب أن نعلمه أن خوارزميات التنقيب في البيانات أو تخزينها أو تحليلها لا تقتصر فقط على رسم شخصية المستخدمين، بل تستهدف أيضاً اهتماماتهم الشخصية من خلال مراقبة السلوك الإلكتروني وكيفية استخدامه للبيانات في مختلف المجالات خصوصاً الجوانب الشخصية (عبد المطلب, ممدوح عبد الحميد, 2020; عيسى, 2019). فلا توجد ضوابط لاستخدام هذه التقنية أو تطويرها، يقول مايك شروبفر الرئيس التنفيذي للتطوير في فيسبوك" أن تقنيات التزييف العميق تتطور بسرعة؛ لذا هناك حاجة ماسة للعمل على إنتاج وسائل أفضل لكشف التزييف" (Knight, 2020). ويعني ذلك أن هذه التقنية قد تفرض تحديات حقيقية أمام أجهزة العدالة الجنائية (Liu & Mazibrada, 2020; محرم, 2022)، ومن المسائل الشائكة في هذا الجانب صعوبة تحديد المسؤول جنائياً عن سلوك التلاعب في المحتوى الرقمي لا سيما إذا ارتكبت الجريمة من الآلة الذكية ذاتها أو بالأخرى عن طريق خوارزميات الذكاء الاصطناعي التي أتمتة الآلة بحيث تؤدي العمل دون تدخل من الإنسان ذاته، فضلاً عن صعوبة إثبات ما إذا كان هناك تدخلٌ فعلاً من الأخير أو عدمه (Hallevy, 2015; الأسيوطي, 2020)، كذلك قد تؤثر في تقدير الدليل أمام المحاكم

وباعتقادنا أن المنظم الصيني عندما استعان بلفظ التوليف العميق كان قاصداً التمييز بين مشروعية استخدام هذه التقنية وعدم مشروعيتها والتي يشار إليها بلفظ التزييف العميق.

المطلب الثاني: الطبيعة القانونية لسوء استخدام تقنية التوليف العميق (التزييف العميق)

لما كانت هذه التقنية تعتمد بشكل أساسي على أدوات تقنية المعلومات كأجهزة الحاسب الآلي والهواتف المحمولة إذ لا يمكن تصور تحقق الإساءة إلا من خلال تلك الأدوات، فإنها تعد نموذجاً للجرائم السيبرانية التي اختلف الفقهاء والقوانين أيضاً حتى يومنا هذا على إيجاد مصطلح ومفهوم جامع ومانع لها حتى أن بعض الباحثين وصفها بأزمة المصطلح والمفهوم (المناعسة & الزعبي, 2014)، ومن ناحيتنا نرى أن المصطلح الأنسب هو مصطلح جرائم تقنية المعلومات الذي استخدمته الاتفاقية العربية لمكافحة جرائم تقنية المعلومات، أو مصطلح الجرائم السيبرانية إذا أردنا ترجمته من اللغة الإنجليزية Cybercrime كما هو الحال في اتفاقية بودابست الأوروبية الصادرة عام 2001 فقد تبنت كافة الدول الأوروبية مصطلح الجرائم السيبرانية.

أما تعريفاتها فنجد أن التعريف الأشمل هو الذي يعرض أدوات تكنولوجيا المعلومات كوسائل أو أدوات لتنفيذ النشاط الإجرامي عبرها أو هدفٍ لها أو بيئة حاضنة للمحتوى الإجرامي (Clough, 2015; فكري, 2007). فهذا التعريف يجمع الأنشطة المستحدثة والأنشطة التقليدية، كما نرى أنه قادرٌ على استيعاب ما يقدمه المستقبل من نماذج أخرى بما في ذلك الأنشطة الإجرامية عبر الذكاء الاصطناعي التي غيرت طبيعة هذه الجرائم ومفهومها فقد جعلتها أكثر خطورة من قبل حيث لم تعد إلكترونية فحسب؛ بل أصبحت جرائم ذكية. وتفسير هذه النقلة النوعية أن الأداة التكنولوجية شبهة مؤتمتة أي أن الإنسان بوصفه المستخدم هو الذي يتحكم باستخدامها لتؤدي الأداة عملها بموجب تعليماته، على خلاف الوضع الآن فإن الذكاء الاصطناعي منح الأدوات القدرة على اتخاذ القرار دون تدخل المستخدم ذاته. والسؤال الذي نطرحه في سياق هذا المطلب ما النماذج الإجرامية التي يمكن أن ترتكب باستخدام تقنية التزييف العميق؟

1. **أنشطة الاحتيال:** إن المحتوى الرقمي للأشخاص المنشور في شبكة الإنترنت مكن المجرمين من الاحتيال عن طريق سرقة هويتهم وانتحال شخصيتهم، بل وإلحاق أضراراً مالية بهم باستخدام تقنية التزييف العميق القائمة على الذكاء الاصطناعي؛ إذ يمكن إنشاء روابط مزيفة (Sloot et al., 2021).
2. **أنشطة التنمر أو التهديد والابتزاز أو تشويه السمعة:** يمكن للمجرمين استخدام تلك التطبيقات في التنمر بالآخرين أو تهديدهم وابتزازهم أو تشويه سمعتهم أو الانتقام منهم أو غير ذلك من أنشطة أخرى تشكل خطراً على أمن مستخدمي التكنولوجيا ومن بين هذه النماذج نشر رسائل تهديد أو نشر المحتوى الإباحي (Mustak et al., 2023).

3. **أنشطة انتهاك الملكية الفكرية:** قد يترتب على هذه الأنشطة انتهاك لحق الملكية الفكرية سواء كان المحتوى يتصل بعمل موسيقى، أو رسومات، أو مقاطع سينمائية، أو مؤلفات، أو غير ذلك من محتوى محمي بموجب القوانين المنظمة لهذا الحق، ويزداد الخوف إذا كان التعلم الآلي بواسطة الذكاء الاصطناعي لتزييف المحتوى كان سبباً لإنشاء المحتوى المزيف؛ إذ يمكن أن يكون المحتوى أشبه بالواقع . (Tyagi, 2023)

4. **أنشطة التضليل:** أثبت الواقع التقني أن الذكاء الاصطناعي قد يشكل إضراراً بأسس الديمقراطية؛ إذ استغل البعض تطبيقات التزييف العميق في التأثير على نزاهة العملية الانتخابية من خلال استهداف المرشحين ومشاركة المحتوى المزيف في شبكة الإنترنت أو شبكات التواصل الاجتماعي (Ray, 2021). وقد قدمنا أن هذه التطبيقات أدت إلى تلاشي مفهوم الحقيقة.

5. **انتهاك حق الخصوصية والحق في الصورة وحق النسيان:** أصبح الكشف عن الخصوصية مسألة مقبولة لدى الكثير من المستخدمين إذ يخاطرون بنشر صورهم أو مقاطع يومياتهم عبر وسائل التواصل الاجتماعي فيتم العبث بالمحتوى المنشور دون موافقتهم (Chesney & Citron, 2019). كما نرى أن العبث بصور أو مقاطع أفراد متوفين قد يشكل تعدياً على الحق في الدخول في طي النسيان.

ويمن القول بأن التزييف العميق من بين العوامل التي ساهمت في ازدياد معدل الجرائم السيبرانية خصوصاً مع اعتماد هذه التقنية على خوارزميات الذكاء الاصطناعي؛ إذ يمكن إنشاء محتويات مزيفة لتنفيذ العديد من الجرائم السيبرانية على النحو السالف ذكره، وقد أظهرت نتائج استطلاعية صدرت في أغسطس 2022 أن 66 % من المتخصصين في الأمن السيبراني الذين شملهم الاستطلاع شهدوا استخدام التزييف العميق كجزء من هجوم إلكتروني، ويمثل ذلك زيادة بنسبة13 %على أساس سنوي، حسبما ذكرته شركة VMware في تقريرها السنوي الثامن عن التهديدات المتعلقة بالاستجابة للحوادث العالمية، وكان البريد الإلكتروني هو طريقة التسليم المستخدمة في 78 % من تلك الهجمات (VMware, 2022). ونؤيد ما ذهب إليه البعض من أن هذه التقنية تمثل تهديداً حقيقياً للأمن السيبراني. ففي الصين كشف أحد التقارير عن نسبة تعامل المحاكم الصينية مع القضايا المرتبطة في الفضاء السيبراني؛ إذ تعاملت في الفترة ما بين 2017 حتى 2021 مع أكثر من 282 ألف جريمة مختلفة، وقد احتل الاحتيال النسبة الأعلى بنسبة 36.53 % تركزت على القروض الوهمية وانتحال الشخصية والتوظيف الزائف (van Wyk, 2022).

وقد أبدت محكمة الشعب العليا في الصين (SPC) رأيها في الفتوى الصادرة بتاريخ 8 ديسمبر 2022 بشأن تنظيم وتعزيز الذكاء الاصطناعي في الممارسات القضائية بقولها:

"يتعين على محاكم الشعب أن تتبنى أساليب شاملة، بما في ذلك المراجعات الأخلاقية ومراجعات الامتثال والتقييمات الأمنية، لمنع وتخفيف مخاطر الأمن السيبراني في تطبيقات الذكاء الاصطناعي القضائية" (Chinese Supreme People's Court, 2022)

المبحث الثاني: موقف القوانين الجنائية المقارنة من أفعال التزييف العميق

اتجهت بعض قوانين الدول إلى مواجهة أنشطة التزييف العميق من خلال تجريم أنشطتها بنصوص خاصة كما هو الحال في القوانين الجنائية الأمريكية في الولايات المختلفة، بينما اتجهت قوانين أخرى إلى إخضاع هذه الجرائم إلى القوانين المعنية بمكافحة الجرائم السيبرانية أو المدونة السيبرانية ومثلها دولة الإمارات العربية المتحدة.

المطلب الأول: مواجهة التزييف العميق في القانونين الأمريكية

حظر المشرع الأمريكي هذه الأنشطة على المستويين المحلي والفيدرالي. فعلى المستوى الفيدرالي صدر أول تشريع في ديسمبر 2019 بعد إقراره من مجلس الشيوخ ونفاذه في 2020 ليكون جزءًا من أقسام قانون تفويض الدفاع الوطني متضمناً التزييف العميق؛ إذ اعتبر المشرع الفيدرالي أن التزييف العميق مشكلة تتعلق بالأمن القومي (Ferraro et al., 2020). والجدير ذكره أن هناك مشروعين قانونيين- يتعلقان أيضاً في الموضوع ذاته- لا يزالان في غرف الكونغرس (Chipman & Preston, 2019)

وقد احتوى القسم 5709 من هذا القانون على ثلاثة بنود أساسية أولها هو إلزام الاستخبارات الوطنية بتقديم تقرير شامل سنوياً إلى الكونغرس حول مسائل التسليح الأجنبي للتزييف العميق، وبمعنى آخر تقديم تقرير يتضمن التأثيرات المحتملة أو الفعلية وخطورتها على الأمن القومي بسبب المحتوى المتلاعب فيه عن طريق هذه التقنيات في وسائل الإعلام والتي قد تستخدمها حكومات أجنبية لنشر معلومات مضللة أو الانخراط في أنشطة خبيثة أخرى. وفي البند الثاني ألزم المشرع الحكومة بإخطار الكونغرس عن الحملات التي تتضمن أنشطة تضليل للمحتوى والتي تستهدف الانتخابات الأمريكية أو العمليات السياسية الداخلية من قبل أي دولة أو كيان أو فرد أجنبي. وأما الثالث فقد تناوله القسم رقم 5724 وتناول فيه المشرع منح جوائز تنافسية قد تصل إلى 5 ملايين دولار أمريكي لتحفيز البحث العلمي أو تطوير آليات أو تسويق تقنيات تساعد على الكشف تلقائيًا عن المحتوى الذي يتم التلاعب بها آليًا (Chipman & Preston, 2019)

وقد واجهت بعض قوانين الولايات أنشطة التزييف العميق في نطاق محدد أي في نطاق واقعة معينة. فقد صدر عن ولايتي كاليفورنيا وتكساس عام 2019 أول قانونين داخليين يتعلقان بمكافحة أنشطة التزييف العميق أثناء سير العمليات الانتخابية (Westerlund, 2019; فاضل & عباس, 2022; محرم, 2022). وبموجب قانون كاليفورنيا فقد حظر القانون (AB730) التلاعب بالمحتوى الرقمي الخاص بالمرشحين السياسيين والكشف عنه أو نشره خلال 60 يوماً من الانتخابات بقصد الإضرار بسمعة المرشح أو لخداع الناخب ليصوت لصالح المرشح أو ضده، وما يترتب على ذلك إرباك للناخبين عند التصويت، وقد اقتصر المشرع على ترتيب المسؤولية المدنية دون غيرها متى تثبت الضرر عملاً بنص المادة 35 من قانون الإجراءات المدنية، فلا يجوز تقييد أو تجريم هذا السلوك مهما كان مضللاً خصوصاً في هذه الفترة كون ذلك يتعارض مع مبدأ حرية التعبير وما يضمن من حرية في الخطابات السياسية خلال فترة الانتخابات المنصوص عليها في التعديل الأول من الدستور الأمريكي الرأي (Langa, 2021)وأيضاً ما أقرته المحكمة العليا الأمريكية حيث قالت" أن خوف الولاية من أن الناخبين قد لا يختارون الحكيم لا يوفر للدولة مبررًا مقنعًا لتقييد حرية التعبير" (U.S. Supreme Court, 1982). لذلك أبطلت المحكمة العليا العديد من المحاولات لحظر الأنشطة التي قد تكون فعلاً نموذجاً للتزييف العميق (Tashman, 2021) والحال كذلك في القانون AB602)) الخاص بحظر أنشطة التزييف العميق المتضمنة مواد إباحية ونشرها أو إتاحتها عمداً بدون رضى حيث لم يفرض عقوبات جزائية عليها واكتفى بالتعويض المالي بحد أقصى 150.000 دولار ولا تقل عن 1500 دولار.

والجدير ذكره أنه كان هناك محاولة من خلال مشروع قانون رقم (AB1280) تم تقديمه في فبراير2019 لتجريم أنشطة التزييف العميق لمدة عام واحد في سجن المقاطعة لكل من يعد أو ينتج أو يكشف عن محتوى مزيف تم تقديمه، وما يميز هذا المشروع أنه توسع في بيان أنشطة التجريم وليس كما هو الحال في القانونين السابق ذكرهما واللذان يقتصران على سلوك الكشف، كما أن هناك حاجة له خصوصاً مع استغلاله ضد الأطفال، إلا أن هذا المشروع لم ينجح كونه يتعارض مع التعديل الأول من الدستور وأن عقوبة السجن تعد قاسية جداً (Vazquez, 2021).

أما ولاية تكساس فكانت على خلاف ما قررته ولاية كاليفورنيا؛ إذ قرر قانونها (TXSB 751) الخاص بالجرائم الانتخابية الصادر في العام ذاته معتبراً سلوك إنشاء مقاطع مزيفة باستخدام تطبيقات التوليف أو نشرها خلال 30 يوماً من الانتخابات بقصد الإضرار بالغير أو التأثير على سير العملية الانتخابية، فقد قرر أنها جنحة من الدرجة الأولى وعقوبتها السجن مدة تصل إلى عام وغرامة 4000 دولار أو كلاهما. والوصف ذاته والعقوبة قررتها (TXSB1361) فيما يتعلق بتجريم المواد الإباحية المزيفة، كما جرم سلوك التنمر باستخدام

التزييف العميق بموجب (SB 530) التي أصبحت نافذة منذ 2021 حيث اعتبرت التنمر باستخدام هذه التقنية جنحة من الدرجة الثانية وعقوبتها السجن مدة تصل إلى 180 يوم وغرامة 2000 دولار. وإذا كان القصد من التلاعب التحرش جنسياً فالعقوبة تكون بموجب القسم 42.7 من قانون العقوبات التي تقرر الجنحة من الدرجة الثانية وعقوبتها السجن مدة تصل إلى 180 يوم وغرامة 2000 دولار فضلاً عن الحرمان من الحصول على ترخيص سلاح لمدة خمسة سنوات. وإذا كان القصد منها الابتزاز فإن العقوبة تختلف بحسب ما هو منصوص عليه في القسمين 31.03 و31.02 من قانون العقوبات حيث تتدرج العقوبة بحسب القيمة إذا كانت القيمة محل الابتزاز أقل من 100 دولار فإن العقوبة هي جنحة من الدرجة الثالثة وإذا كانت أكثر من ذلك قد تصل إلى أقصى حد السجن مدى الحياة وغرامة مالية بقيمة 10.000 دولار (Varghese, 2023)

وفي ولاية فرجينيا صدر قانون عام 2019 أُطلق عليه قانون الإباحية الانتقامية حيث جرم فيه أنشطة نشر المحتوى الإباحي المزيف دون موافقة الغير بقصد الإكراه، أو المضايقة، أو الترهيب، أو بيع المحتوى المزيف، وذلك في القسم (18.2-386.2)، وقد اعتبرها المشرع جنحة من الدرجة الأولى المعاقب عليها بالسجن تصل لمدة عام وغرامة 2.500 دولار (Vazquez, 2021). كذلك جرمت ولاية نيويورك مؤخراً النشاط ذاته بموجب مشروع قانون رقم ((S1042A المعدل للقسم 245.15 من قانون العقوبات؛ إذ عاقبت مرتكبها بالسجن مدة عام وغرامة 1000 دولار كما مكنت الضحايا من متابعة الإجراءات القانونية ضدهم (Hinchey et al., 2023).

والجدير ذكره أن القوانين المجرمة لم تشر بوضوح إلى مسؤولية مزود الخدمات للتطبيقات ذاتها -كما هو الحال في الصين- بل أن المشرع في ولاية فيرجينيا نص صراحة في الفقرة ثانية من القانون ذاته أن مزود الخدمات الذي تحقق فيه النشاط المحظور لا يتحمل مسؤولية هذا المحتوى

وعلى الرغم من تصدى القضاء الأمريكي تاريخياً لمسائل عديدة تتعلق بإثبات الأدلة في الجرائم المتعلقة بالتزوير والتزييف، إلا أنها أصبحت تواجه تحديات كثيرة أمام تطور أساليب التزييف العميق خصوصاً مع تطور تقنية الذكاء الاصطناعي؛ إذ ثبت عدم ملاءمة وقدرة قواعد الإثبات المعمول بها سواء في القانون الفيدرالي أو قواعد القانون العام على هذه الوقائع بسبب عدم الوثوق في الأدلة الحالية وفرصة الدفاع في الطعن ضدها وأيضاً شكوك هيئة المحلفين، ففي تعليق لمحكمة الاستئناف في ولاية مشيغين الأمريكية عام 2021 على حكم المحكمة الابتدائية المطعون فيه بشأن قضية تتعلق بنشر محتوى مزيف ضد المجني عليه وربطه بعصابة، بينت فيه أن المحكمة الابتدائية لم تستغل سلطتها التقديرية في التأكد من صحة المنشورات على صفحة فيسبوك قبل تقرير الإدانة وذلك لوجود مخاوف

في موثوقيتها بسبب إمكانية تزييف المحتوى أو اختراق الحساب (Court of Appeals of Michigan, 2021). وفي السياق ذاته أقرت صراحة محكمة استئناف في ولاية كاليفورنيا عام 2019 في دعوى مدنية بأن "وجود أدلة ملفقة بسهولة مثل تقنية التزييف العميق سيجعل من رفع القضايا بموجب معايير المرافعات الفيدرالية المشددة أكثر صعوبة، إن لم يكن مستحيلاً (District Court C.D. California, 2021)

ويرى البعض أنه إذا كانت المبادئ الأساسية للإثبات في النظام القانوني الأمريكي قد استقرت على أن القضاء وهيئة المحلفين هما الجهتان اللتان يُناط إليهما إثبات الحقيقة بناء على الأدلة، فإنه لابد من منحهما المرونة في تقدير الأدلة وتطوير مهاراتهما في الكشف عن الحقيقة خصوصاً مع التطور التكنولوجي الذي سهل إنشاء أدلة سوف تعيق أداء مهام المحكمة (Delfino, 2023)

والجدير ذكره أنه منذ عام 2018 قدمت مقترحات تشريعية فيدرالية، ولكنها لم تمرر وكان أهم هذه المقترحات مشروع قانون H.R. 3230 الخاص بمكافحة التزييف العميق، والذي فرض عقوبات جنائية ومدنية على المخالفين، وقد وضع هذا المشروع التزاما بوضع علامات مائية رقمية وعلامات مكتوبة أو بارزة توضح التعديل الذي أجري على المحتوى الحقيقي على سبيل المثال، يقوم تطبيق Truepic في أجهزة الهواتف المحمولة بختم علامة مائية رقمية على كل صورة يتم التقاطها بكاميرا ذلك الجهاز المحمول. وهذه العملية وإن كانت جيدة في واقع الأمر إلا أنه لا يمكن أن تكون هذه فعالة بدون إنشاء بيئة إلزامية كاملة للأجهزة وبرامج للكاميرات الرقمية وتطبيقات التحرير (Delfino, 2023)، وهو ما قامت به الصين في اللائحة الخاصة بالتوليف العميق.

المطلب الثاني: النموذج الإماراتي في تجريم التزييف العميق

ساير المشرع الإماراتي الاتجاه العالمي لتطوير المنظومة الإدارية والخدماتية في العالم السيبراني، فقد وضعت الحكومة الاتحادية لوائح عديدة تحاكي التطور الرقمي وشملت عدة أدلة أولها دليل أخلاقيات الذكاء الاصطناعي، واستراتيجية استخدامه حتى عام2031، ودليل البنية التحتية لتطبيقاتها المختلفة، ودليل خاص للتعاملات الرقمية وشمل أيضاً دليلاً للتزييف العميق، كما وضعت تقريراً لحوكمة الميتافيرس (حكومة الإمارات العربية المتحدة, 2022).

وهذه الصحوة الإرشادية دفعت المشرع الاتحادي إلى إصدار مرسوم اتحادي جديد يتلاءم مع واقع التطور التقني وهو المرسوم الاتحادي رقم 34 لسنة 2021 في شأن مكافحة الشائعات والجرائم الإلكترونية، وأصبح نافذاً في 2 يناير 2022. وقد خصص

المشرع أحكاماً جديدة تتصل بشكل مباشر وغير مباشر بسوء استخدام تقنية التوليف العميق. فالمشرع الإماراتي اعتبر أفعالها نموذجاً حديثاً من الجرائم السيبرانية التي بدأت تعتمد مؤخراً على الذكاء الاصطناعي.

والحقيقة أن هناك نصوص عديدة يمكن تطبيق أحكامها على أفعال التزييف العميق وذلك متى توافرت شروطها إلا أننا سوف نركز على بعضها، وهي على النحو الآتي:

تناول المشرع في المواد من 52 وحتى 55 فصلاً يُعني بتجريم نشر الشائعات والأخبار الزائفة، فقد جرم المشرع في (المادة 52) نشر الشائعات والأخبار الكاذبة؛ إذ عاقب عليها بالحبس مدة لا تقل عن سنة والغرامة لا تقل عن 100,000 ألف درهم إذا كان في الأوقات العادية، لكن العقوبة تصل للحبس مدة لا تقل عن سنتين والغرامة التي لا تقل عن 200,000 ألف درهم في زمن الأوبئة والأزمات أو الكوارث. وفي (المادة 53) جرم المشرع إتاحة محتوى غير قانوني والامتناع عن أوامر إزالته بالغرامة التي لا تقل عن 300,000 ألف درهم ولا تزيد عن 10,000,000 ملايين درهم. وفي (المادة 54) جرم المشرع إنشاء أو تعديل روبوتات إلكترونية لنقل بيانات زائفة في الدولة، وعاقب عليها بالحبس مدة لا تزيد عن سنتين والغرامة 100,000 ألف درهم ولا تزيد عن 1,000,000 مليون درهم. وجاءت (المادة 55) لتجرم الحصول على عطية لنشر محتوى غير قانوني أو بيانات زائفة، وقرر المشرع إنزال عقوبة السجن المؤقت والغرامة التي لا تزيد عن 2,000,000 مليون درهم.

وجرم المشرع أيضاً سلوكيات عديدة مثل جريمة العبث بالأدلة الرقمية من قبل المسؤول عن إدارة الموقع، أو الحساب، أو البريد الإلكتروني، أو النظام في (المادة 18) وعاقب عليها بالحبس مدة لا تزيد عن ستة أشهر والغرامة التي لا تقل عن 200,000 ألف درهم أو بإحدى هاتين العقوبتين. كما جرم المشرع في (المادة 19) كل مسؤول عن إدارة موقع أو حساب نشر فيها بيانات أو معلومات لا تتوافق مع معايير المحتوى الإعلامي المنصوص عليها، وعاقب عليها بالحبس مدة لا تزيد عن سنة والغرامة التي لا تقل عن 30,000 ألف درهم ولا تزيد عن 300,000 درهم، أو بإحدى هاتين العقوبتين.

وقد اعتبر المشرع في (المادة 65) الأدلة المستمدة أو المستخرجة من الأنظمة الإلكترونية أو برامجها أو أي وسيلة أخرى لها حجية الأدلة الجنائية المادية في الإثبات الجنائي، وكنا نأمل أن يتناول المشرع شروط صحة الدليل الإلكتروني حتى تكون حجيته بذات قوة الدليل التقليدي لا سيما مع إمكانية العبث به بسهولة باستخدام الذكاء الاصطناعي. وأيضاً أن تشمل أوامر التصحيح والإيقاف والتدابير الأخرى كل الجرائم المتصلة بالمحتوى وليس فقط الجرائم المنصوص عليها في (المادة 71) من المرسوم والتي اقتصرت على

الجرائم الماسة بأمن الدولة. فكل التدابير من وجهة نظرنا مستحق تطبيقها على كافة الجرائم طالما كانت تنتهك حقوق الآخرين.

وما يميز هذا المرسوم عن المراسيم الأخرى السابقة أن المشرع الإماراتي بين في (المادة 69) من المرسوم امتداد نطاق تطبيق أحكامه إلى خارج نطاق إقليم الدولة، وذلك في حالات محددة أولها إذا كان محل الجريمة نظام، أو شبكة، أو وسيلة معلوماتية، أو موقع إلكتروني عائد لإحدى مؤسسات الدولة. وإذا تم الإعداد للجريمة أو المساهمة فيها في الدولة. وإذا كان من شأن الجريمة المساس بأمن الدولة في الداخل أو الخارج أو بأي مصلحة من مصالحها، أو إلحاق الضرر بأي من مواطنيها أو المقيمين فيها. وإذا وجد مرتكب الجريمة في الدولة، بعد ارتكابها ولم يتم تسليمه.

المبحث الثالث: المسلك الصيني في مواجهة أفعال التزييف العميق

لم تختلف رغبة الصين عن غيرها من الدول في مواجهة الأنماط الإجرامية المستحدثة ومن بينها سوء استخدام تقنية التوليف العميق، وقد انفردت الحكومة بوضع لائحة إدارية تعاونت فيها إدارة الفضاء الإلكتروني الصينية ووزارة الصناعة وتكنولوجيا المعلومات ووزارة الأمن العام على وصياغت أحكامها التي تجسدت بـ 25 مادة أصبحت نافذة في يناير 2023.

المطلب الأول: لائحة خدمات التوليف العميق واللوائح الإدارية الأخرى المنظمة للبيئة السيبرانية

جاءت هذه اللائحة كاشفة لغاية المنظم في تنظيم خدمات التوليف العميق، وقد بينت المادة الأولى من اللائحة بأن صياغة هذه الأحكام إنما هي قائمة على أساس مجموعة من القوانين واللوائح الإدارية، وتتمثل في قانون الأمن السيبراني، وقانون أمن البيانات، وقانون حماية المعلومات الشخصية، والتدابير الخاصة بإدارة خدمات معلومات الإنترنت، والقوانين واللوائح الإدارية الأخرى ذات الصلة، من أجل تنظيم أنشطة التوليف العميق لخدمات معلومات الإنترنت، للارتقاء بالقيم الاشتراكية الأساسية، والحفاظ على الأمن القومي والمصلحة العامة المجتمعية، وحماية الحقوق والمصالح المشروعة للمواطنين والأشخاص الاعتباريين والمنظمات الأخرى (Chinese Congress, 2020)

وهذا النص يوضح توسع الصين في منح المنظم إصدار لوائح تنظيمية لمعالجة المخاطر في البيئة السيبرانية بما في ذلك استخدامات الذكاء الاصطناعي، وقد تضمنت هذه اللوائح أحكاماً تنشئ التزامات الامتثال على الكيانات العاملة في الأعمال المتعلقة بالذكاء

الاصطناعي وحوكمة آلياتها منذ بداية القرن الحادي والعشرين (Sheehan, 2023). ويرى بعض الباحثين أن هذا النسيج الحاصل بين القواعد القانونية والتنظيمية قد أثبت فاعليته في دعم سياسة المشرع والقضاء للمحافظة على الأمن والاستقرار على مستوى المجتمع والدولة (Li, 2015). وترتيباً على ذلك، فقد أصدر المنظم الصيني عدة لوائح تنظيمية تتعلق بتدابير إدارية خاصة بإدارة المحتوى الرقمي وتنظيم أعماله مثل التدابير الإدارية بشأن أمن خدمات معلومات الإنترنت الصادرة عام 2000 والتدابير المتعلقة ببرامج الفيديو والصوت عبر شبكة الإنترنت، وقد صدرت من المكتب العام للإذاعة والتلفزيون عام 2004، والتدابير الإدارية بشأن إدارة خدمات المعلومات الصوتية والمرئية عبر الإنترنت الصادرة عام 2019 وهذه التدابير جاءت لمواجهة نشر الأخبار المزيفة" الشائعات" (Hine & Floridi, 2022).

هذا بالإضافة إلى لوائح إدارية أخرى تنظم أحكاماً لاستخدامات تقنية الذكاء الاصطناعي وترتبط بلائحة التوليف العميق كاللائحة الخاصة بإدارة توصيات الخوارزميات في خدمات المعلومات على شبكة الإنترنت الصادرة في عام 2022، ولائحة الذكاء الاصطناعي التوليدي الصادرة في عام 2023، وهناك أيضاً لائحة خاصة جديدة صدرت العام ذاته وما زالت قيد المراجعة والمشاورات العامة وتتعلق بالتدابير الأخلاقية لأنشطة العلوم والتكنولوجيا (Sheehan, 2023)

وفيما يتعلق بالالتزامات التي أنشأها المنظم الصيني في لائحة خدمات التوليف العميق، فقد جاءت بحزمة من الالتزامات الموجهة في مجملها إلى مقدمي الخدمات(Hine & Floridi, 2022) من أجل التأكيد على الغاية التي بينها المنظم في المادة الأولى. فما هي تلك الالتزامات التي وردت في هذه اللائحة؟ وهل فرضت عقوبات على مخالفتها؟

أوردت اللائحة العديد من الالتزامات التي تغطي مجالات فنية وأخلاقية يتوجب على المزودين تحديداً والمستخدمين اتباعها وتجنب محاذيرها (Chinese Congress, 2020). ونلخص أهم هذه الالتزامات على النحو الآتي:

1. الالتزام بتحقيق معايير أمن المحتوى، وذلك من خلال إجراء تقييمات أمنية لسلامة المحتوى عند توفير النماذج والقوالب والأدوات الأخرى مع وظيفة تحرير الوجه والصوت وغيرها من القياسات الحيوية وأيضاً المعلومات أو الأشياء غير البيوميترية التي قد تتعلق بالأمن القومي والصورة الوطنية والمصالح الوطنية والمصالح العامة.
2. الالتزام بالشفافية من خلال وضع إرشادات ومعايير وعمليات للتعرف على المعلومات الخاطئة أو الضارة، والتعامل مع المستخدمين الذين ينتجون مواد كاذبة

أو ضـارة باسـتخدام تقنيـة التوليـف العميـق. وقـد اشـترطت اللائحـة شـرطاً أساسـياً لمشـروعية المحتـوى موضـوع التوليـف عنـد إنشـاء المحتـوى المتلاعـب فيـه وضـع ملصـق أو علامـة مائيـة، وتشـمل ذلـك المحـاكاة الصوتيـة أو المحادثـة الذكيـة أو الكتابـة التـي تحاكـي أسـلوب الشـخص الحقيقـي أو تركيـب صـورة الوجـه أو التلاعـب بالوجـه.

3. الالتـزام بتشـكيل قواعـد الإدارة واتفاقيـات النظـام الأساسـي والكشـف عنهـا، وتحسـين اتفاقيـات الخدمـة، وتنفيـذ نظـام مصادقـة معلومـات الهويـة الحقيقيـة بحيـث يسـهل تحديـد منشـئ المحتـوى، وهـذا بطبيعـة الحـال يتطلـب تسـجيلهم فـي التطبيـق.

4. الالتـزام بإنشـاء آليـة لتبديـد الأخبـار المزيفـة والشـائعات بحيـث إنـه عنـد اسـتخدام خدمـات التوليـف العميـق لإنتـاج معلومـات كاذبـة ونسـخها ونشـرها، يُطلـب مـن مقدمـي الخدمـات اتخـاذ تدابيـر لتبديـد مثـل هـذا المحتـوى، والاحتفـاظ بالسـجلات، وإبـلاغ الجهـات المختصـة عنهـا.

فلا يجـوز لأي منظمـة أو فـرد اسـتخدام خدمـات التوليـف العميـق فـي مخالفـة مـا ورد مـن التزامـات حرصـت الصيـن علـى عـدم انتهاكهـا، وقـد وردت المحظـورات فـي المـواد مـن 4 حتـى 7 مـن حقـوق وقيـم للأفـراد والدولـة قـد يعـرض المسـاس بهـا تقويـض الأمـن والمصالـح القوميـة للخطـر، أو الإضـرار بالصـورة الوطنيـة، أو التعـدي علـى المصالـح العامـة، أو تعطيـل النظـام الاقتصـادي والاجتماعـي، أو التعـدي علـى الحقـوق والمصالـح المشـروعة للآخريـن.

فهـذه الالتزامـات مـن شـأنها أن تحـد من التهديـدات المسـتقبلية في البيئـة السـيبرانية خصوصـاً مـع دخـول الـذكاء الاصطناعـي- كمـا وضحنـا سـابقاً- فـي تطويـر تطبيقاتهـا، فالصيـن علـى الرغـم مـن عـدم قدرتهـا علـى فـرض السـيطرة الكاملـة علـى المحتويـات المخالفـة فـي شـبكة الإنترنـت والتـي يمكـن إنشـاؤها بطبيعـة الحـال خـارج الأقاليـم الصينيـة، إلا أنهـا مازالـت تحـاول إحـكام الفوضـى فـي المحتـوى الـذي يتـم تداولـه فـي بيئـة الإنترنـت مـن بوابـة إلـزام مـزودي الخدمـات.

وقـد لاحظنـا أن اللائحـة ذاتهـا لـم تحـدد أي عقوبـات لعـدم الامتثـال أو الإخلال بالالتزامـات الـواردة فـي اللائحـة، وقـد بينـت المـادة 22 مـن اللائحـة جـواز فـرض العقوبـات المقـررة فـي القوانيـن واللوائـح الإداريـة الأخـرى المعمـول بهـا فـي حـال انتهـاك أي مـزود خدمـة التوليـف العميـق أو الداعـم الفنـي أو المسـتخدمين لأحـكام اللائحـة وثبـوت مسـؤوليتهم الجنائيـة.

ومـع ذلـك، فهـي تمكـن الجهـات التـي حددتهـا اللائحـة مـن الإشـراف علـى امتثـال مـزودي الخدمـات والداعميـن الفنييـن بأحكامهـا وإجـراء التفتيـش علـى عمليـات التوليـف العميـق. ويجـوز لهـا بموجـب صلاحياتهـا أن تأمرهـم بتعليـق تحديثـات المعلومـات أو تسـجيل حسـاب المسـتخدم

أو الخدمات الأخرى، وإجبارهم على إجراء تصحيح أي مخالفة لعدم امتثال بما في ذلك إزالة التطبيق.

المطلب الثاني: سياسة الصين في تجريم أفعال التزييف العميق

طالما كانت أدوات تقنية المعلومات وسيلة اعتداء أو محلاً أو هدفاً لها، فبلا شك أن اعتداءاتها تخضع لمفهوم الجرائم السيبرانية، وفي الصين اشتهرت هذه الجرائم بمسمى جرائم الشبكة (Li, 2015). وقد بدأت بمواجهتها عندما أصدر مجلس الدولة مرسوم رقم 147 لسنة 1994 الخاص بالحماية الأمنية لنظام المعلومات الحاسوبية؛ إذ أورد فيها أحكاماً لتجريم هذه الأنشطة في إطار المادة 24 من قانون العقوبات القديم الصادر سنة 1979 إلا أن أحكامه لم تكن كافية لمواجهة هذه الجرائم وهذا ما دفع المشرع إلى إصدار قانون عقوبات جديد عام 1997 وإجراء تعديلات عليه بحيث تضمن مواجهة أنماطها المستقبلية كالتزييف العميق الذي ينال من المحتوى المخزن في النظام أي كان شكله. وليس ذلك فحسب؛ بل أن سياسة الصين في مواجهة الجرائم السيبرانية تعتمد أيضاً على الجهود التي تبذلها الحكومة من خلال لوائح أو توجيهات إدارية تنظم الاستخدام وتحدد الالتزامات وتبين المحظورات. إضافة إلى السوابق القضائية التي يمكن الاستئناس بها قبل إصدار الحكم، فقد صدر عن المحكمة العليا تفسيرات عديدة حول الجرائم السيبرانية (Wang, 2016)

ونتيجة للتحديات التي فرضتها هذه الجرائم أصدرت اللجنة الدائمة لمجلس النواب الصيني قراراً شاملاً للحفاظ على أمن الحواسيب عام 2000 لدعم قانون العقوبات (Yong, 2011)، وتم تعديل قانون العقوبات عام 2009 وهو التعديل السابع لهذا القانون بإضافة بعض الجرائم السيبرانية ضمن قانون العقوبات، وشملت المواد 285 و286 و287 ثم صدر قرار بتعزيز حماية شبكة المعلومات والمحتوى عام 2012 ليتم تعديل قانون العقوبات على نطاق أوسع عام 2015 حيث حدد فيه نطاق المسؤولية لمزودي خدمات الإنترنت مضيفاً المواد 286 - 1و287 - 1و287 -(Yong, 2011).

ولما كان التزييف العميق نموذجاً ترتبط أنشطته بالمحتوى المعلوماتي الذي قد يمس العديد من الحقوق والمصالح المحمية كما وردت في المادة الأولى والمواد من 4 حتى 7 من اللائحة والتي أشرنا إليها سابقاً، فإن قانون العقوبات هو القانون الواجب التطبيق فضلاً عن قوانين ولوائح تنظيمية أخرى تحمي حقوقاً ومصالح معينة وتقرر إجراءات إدارية. وسوف نعرض أهم تلك الجرائم وفقاً للترتيب الآتي:

الاحتيال: أصدر المشرع الصيني قانوناً خاصاً لمواجهة هذا النشاط في سبتمبر عام 2022 بسبب ازدياد أنشطته على نحو ما ذكرنا سابقاً، وقد عرف الاحتيال عبر الإنترنت

وشبكات الاتصالات في المادة 2 بأنه "فعل يترتب عليه نقل ممتلكات الآخرين عن بعد أو بطريقة غير معنوية عبر تقنيات الاتصالات والشبكات بغرض الحيازة غير المشروعة". وما يميز هذا القانون أن المشرع في المادة 3 قد وسع من نطاق تطبيق أحكام هذا القانون واختصاصه وقد فسرت المحكمة العليا أن الاختصاص ليس في المكان الذي تحدث فيه نتائج الجريمة، بل يمتد ليشمل المكان حدوث السلوك (Chinese Supreme People's Court, 2016). وقد خصص المشرع المواد من 38 حتى 44 للعقوبات التي تتفاوت بين السجن بمدد متفاوتة قد تصل إلى مدى الحياة والغرامة المالية التي تصل إلى خمسة ملايين يوان والمصادرة فضلاً عن عقوبات لعدم الامتثال لأوامر التصحيح. فضلاً عن عقوبات إدارية ومدنية يمكن إيقاعها على مزودي الخدمات.

إساءة السمعة (التشهير): جرم المشرع الصيني في المادة 246 من قانون العقوبات كل سلوك من شأنه المساس بسمعة الأفراد أو التشهير بهم عن طريق التلاعب بمحتوى أو معلومات كاذبة ونشرها بأي طريقة بما في ذلك شبكة الإنترنت أو حسابات التواصل الاجتماعي، بأنه يعاقب بالسجن مدة تصل إلى ثلاث سنوات، أو إخضاعه للاعتقال الجنائي، أو المراقبة العامة، أو الحرمان من الحرية السياسية. وفي ذلك تقول محكمة العليا في تفسير مشترك مع النيابة العامة بشأن التشهير عبر الإنترنت عام 2013 أنه إذا تم النقر على المحتوى الكاذب أو مشاهدته أكثر من 5000 مرة، أو إعادة توجيهه أكثر من 500 مرة، تعد خطراً بما فيه الكفاية (China Law Translate, 2013).

نشر أخبار زائفة (شائعات): جرم المشرع الصيني نشر أخبار زائفة من شأنها الإخلال بالنظام العام من خلال شبكة الإنترنت أو غيرها من وسائل الإعلام، بموجب الفقرة الثانية من المادة 291 المضافة في التعديل التاسع لقانون العقوبات؛ إذ عاقبت على هذه الجريمة بالسجن لمدة لا تزيد عن ثلاث سنوات أو الاحتجاز الجنائي أو المراقبة العامة. أما إذا كانت مخاطر هذا السلوك جسيمة فإن العقوبة هي السجن لمدة لا تقل ثلاث سنوات ولا تزيد عن سبع سنوات (Zhang, 2019). وبينت المادة 1-286 المضافة بالتعديل ذاته إلى معاقبة مزودي الخدمات عن مخالفة التدابير كعدم تسجيل الأسماء الحقيقية وعدم الامتثال بتصحيح المخالفات وإلى غير ذلك (Li, 2015). كذلك حظر هذا السلوك في الفقرة 2 من المادة 12 من قانون الأمن السيبراني وقد أشارت إلى أن خطورة هذا السلوك ليس فقط الإخلال، بل تناولت آثار عديدة ماسة بحقوق ومصالح الأفراد والمجتمع والدولة. وقد فرض هذا القانون بموجب المواد من 59 حتى 69 غرامات مالية قد تصل إلى 1,000,000 مليون يوان وعقوبات إدارية أخرى.

التزييف في إطار المواد الإباحية: يسعى المشرع الصيني إلى حماية القيم الأخلاقية والثقافية ومنع المظاهر التي تهددها، وقرر العقاب لهذا التعامل في المواد الإباحية بموجب

قانون العقوبات قانون إدارة الأمن العام أيضاً الصادر سنة 2012، إلا أن القانون الأول هو واجب التطبيق حيث جرم في المواد من 363 وحتى 367 من قانون العقوبات أي تعامل يتعلق بمواد إباحية وذلك بإنزال عقوبة السجن مدة لا تقل عن ثلاث سنوات أو وضعه تحت الاحتجاز الجنائي أو المراقبة، بالإضافة إلى الغرامة. أما إذا كانت الجريمة تخص شخصا قاصراً أقل من سن 18 عاماً، فتعد العقوبة مغلظة وقد تصل العقوبة إلى 10 سنوات مع دفع غرامة مالية (Yong, 2011).

انتهاك المعلومات الشخصية والخصوصية: أدخل المشرع هذه الجريمة في التعديل التاسع لقانون العقوبات، وهذا الانتهاك يتحقق عندما يتم المساس بالمعلومات الشخصية للأفراد في البيئة السيبرانية كالصورة على سبيل المثال أو الأصوات أو أي بيانات أخرى ذات طابع شخصي وذلك عن طريق بيعها أو تداولها دون موافقة أصحابها (قرصنة) أو الحصول عليها عن طريق سرقة إذا كان الفاعل موظفاً أو غير ذلك من سلوكيات أدرجها المشرع في إطار المادة 1-253، وقد عاقب عليها المشرع بالسجن مدة لا تزيد عن ثلاث سنوات أو الاحتجاز قصير الأجل والغرامة أو الغرامة فقط، وإذا رتبت آثاراً جسيمة تكون العقوبة السجن لمدة لا تقل عن ثلاث سنوات ولا تزيد عن سبعة سنوات والغرامة، كما تسأل الكيانات المعنوية عن الأضرار المترتبة نتيجة ذلك. وفيما يتعلق بمفهوم الآثار الجسيمة قد بينت المحكمة العليا والنيابة العامة أن تحديدها يكون وفقاً لخمسة معايير وهي كمية المعلومات ونوعها والمكاسب غير المشروعة والمعرفة بالنشاط وصفة القائم بالنشاط وسجله الجنائي (Ridan, 2017).

وفيما يتعلق بإثبات الدليل الرقمي فقد اعترف المشرع الصيني بها منذ تعديل 2012 لقانون الإجراءات الجنائية (Yang & Feng, 2021)؛ إذ عرف الدليل الإلكتروني في المادة 48 منه كنوع جديد من الأدلة (فئة 8) ومستقل عن الأدلة المادية والوثاقية. أما فيما يتعلق بآلية التعامل مع تلك الأدلة فإن المشرع الصيني بسياسته الواسعة جعل أمر التعامل مع الأدلة الرقمية من حيث جمعها وحفظها ومصادقتها في قضايا الجرائم السيبرانية قائماً على لوائح ثلاث اشترك في تفسيرها محكمة الشعب العليا والنيابة الشعبية العليا، وهي لوائح 2014، وأحكام 2016، وقواعد 2019.

وإذا كانت هذه الوثائق شاملة بحيث يمكن التعامل مع قضايا الجرائم السيبرانية وتقدير حجية الدليل الإلكتروني في إثبات وقائعها. إلا أنه في واقع الأمر لا يعد ذلك كافياً لمواجهة أنشطة التزييف العميق خصوصاً مع ظهور خوارزميات الذكاء الاصطناعي التي غيرت قواعد اللعبة، فقد أصبح من الصعب التنبؤ بسلامة المحتوى في المستقبل (Verdoliva, 2020)، وهو بطبيعة الحال يشكل تحدياً حقيقياً أمام أجهزة العدالة الجنائية في تقدير مدى صحة الدليل المستمد من هذه الجرائم.

فعلى الرغم من التسليم بقيام المنظم الصيني بإلزام مزودي الخدمات بضرورة وضع علامة مائية على المحتوى الذي يتم التلاعب فيه باستخدام الذكاء الاصطناعي وهي طريقة فنية ذكية لرصد المحتوى المزيف والتمييز بينه وبين المحتوى الحقيقي، إلا أنها من الناحية العملية قد تكون إجراءً وقتياً قد تتغير فيه قواعد اللعبة أيضاً، كما يصعب إلزام كافة المزودين باتخاذ مثل هذا التدبير لا سيما إذا كانوا خارج نطاق إقليم الصين.

الخاتمة

في ختام هذه الورقة فقد توصلنا إلى بعض النتائج والتوصيات نوردها تباعاً على النحو الآتي.

أولاً- أهم النتائج:

1. استخدم المنظم الصيني مصطلح التوليف العميق للتدليل على مشروعية تغيير المحتوى الرقمي سواء كان صوتاً، أو صورة، أو مقطعاً، أو نصوصاً عبر تطبيقات ليست حديثه، بل كانت موجودة وقد تطورت مع اعتمادها على الذكاء الاصطناعي والبيانات الضخمة.

2. أراد المنظم الصيني التمييز بين مصطلح التوليف العميق للتدليل على مشروعية الاستخدام، والتزييف العميق للتدليل على سوء استخدامه حيث استطاع البعض استغلال إمكانياته في ارتكاب أنشطة غير مشروعة قد ترتقي إلى جرائم جنائية.

3. التزييف العميق نموذج للجريمة السيبرانية كون تقنياته تعتمد على المحتوى الرقمي، وقد ازدادت خطورته في الآونة الأخيرة بسبب خوارزميات الذكاء الاصطناعي والبيانات الضخمة التي أفقدتنا القدرة في معرفة الحقيقي والمزيف منها، وتعد أنشطة الاحتيال ونشر الأخبار المزيفة وصناعة المواد الإباحية من أكثر النماذج الإجرامية عبر هذه التقنيات.

4. التلاعب في المحتوى الرقمي باستخدام هذه التقنيات قد يؤثر على قيمة الدليل الإلكتروني وحجيته في الإثبات أمام القضاء، فهذه التقنيات قد تشكل تحدياً حقيقياً أمام أجهزة العدالة الجنائية في تقدير هذا النوع من الأدلة.

5. تتفق جمهورية الصين مع الدول محل المقارنة في مكافحتها للجرائم السيبرانية، ولكنها اختلفت في سياسة المواجهة مع المشرع الأمريكي، فالأول قام بتعديل أحكام قانون العقوبات الصادر عام 1997 واشتراك الحكومة في وضع اللوائح التنظيمية والتوجيهية، ودعم القضاء بسلطة التفسير والحلول والاعتماد على

السوابق القضائية في المعالجة، بينما الثاني واجهها بشكل جزئي على المستوى الفيدرالي، ومواجهة المشرع الوطني في بعض الولايات بسن قوانين خاصة والسبب أن ذلك يتعارض مع اعتبارات تتعلق بحرية الرأي عن التعبير الواردة في التعديل الأول للدستور.

6. تتقارب سياسة دولة الإمارات العربية المتحدة مع جمهورية الصين في آلية المواجهة؛ إذ قامت الحكومة بوضع مبادئ توجيهية للتكنولوجيات الحديثة بما في ذلك التوليف العميق، وهو ما دفع المشرع إلى إلغاء المرسوم اتحادي الخاص بمكافحة جرائم تقنية المعلومات الصادر سنة 2012 واستبداله بالمرسوم اتحادي رقم 21 لسنة 2021 الذي أطلق عليه مصطلحاً آخر وهو مكافحة الجرائم الإلكترونية والشائعات، الذي احتوى على مصطلحات عديدة من بينها البيانات الزائفة.

7. تعد الصين من أوائل الدول التي وضعت لائحة تنظيمية لاستخدام التوليف العميق للحد من سوء استخدام تقنياته، وقد أصبحت اللائحة نافذة في يناير 2023، وألقت هذه اللائحة وأيضاً اللوائح الأخرى عبئاً كبيراً من الالتزامات الفنية والأمنية التي ينبغي مراعاتها من قبل مزودي الخدمات، وقد أحالت مخالفات عدم الامتثال إلى قوانين أخرى تقرر عقوبات جنائية ومدنية وإدارية.

8. هناك لوائح وتدابير إدارية تنظم إدارة المحتوى الرقمي، وهذه اللوائح من شأنها دعم المنظومة القانونية بمختلف موضوعاتها أهمها قانون الأمن السيبراني وقانون البيانات الشخصية. إلا أن المواجهة تضعف إذا كانت المواجهة خارج إقليم الصين؛ إذ يصعب السيطرة على المحتوى الزائف من خارج الإقليم.

9. تبنى المنظم الصيني حلاً فنياً ألزم فيه مزودي الخدمات وضع علامة مائية تمكن المستخدمين من التمييز بين المحتوى الحقيقي والمحتوى المزيف، وعلى الرغم من أنها خطوة ذكية إلا أنها غير كافية إذ قد يمكن استخدام الذكاء الاصطناعي في إزالة العلامة المائية.

ثانياً- التوصيات:

1. نوصي الدول باتباع مسلك المنظم الصيني بإصدار لائحة تنظيمية مماثلة بمسماها الذي يميز بين النشاط المشروع وغير المشروع وأن تتضمن إلزاماً لمزودي الخدمات بمراعاة الجوانب الفنية والأمنية مع وضع ضوابط لتطوير تلك التقنيات وعدم الاكتفاء باللوائح الإرشادية للاستخدام.

2. نوصي المشرعين بضرورة الأخذ بالاعتبار أن هذه النوعية من الجرائم أصبحت أكثر خطورة بسبب الذكاء الاصطناعي، وهذا يستدعي تحديث القوانين المتعلقة بمكافحة الجرائم السيبرانية والأمن السيبراني تماماً كما فعل المشرع الإماراتي.

3. نوصي بمواجهة العجز الدولي في مواجهة حداثة الجريمة وكبح جماح التطور التكنولوجي المستمر مما صعب المهمة أمام أجهزة العدالة الجنائية، لذلك لابد من اجتماع الدول فيما بينها لرسم سياسة دولية تضمن مواجهة فعالة لكافة الأنشطة غير المشروعة في الفضاء السيبراني، إيماناً بأن مواجهة الجرائم السيبرانية تبدأ دولياً قبل المواجهة الوطنية.

4. من الضروري تدريب كوادر العدالة الجنائية والاستمرار في هذا المجال تزامناً مع التطور التكنولوجي لضمان استيعاب خطورتها ووضع الحلول المناسبة للحد من آثارها.

قائمة المصادر والمراجع:

أولاً: المراجع العربية:

إبراهيم, سارة (2021)، كيف تغيّر عمليات "التزييف المتقنة" نظرتنا للواقع. https://www.swissinfo.ch/ara/. Retrieved Nov 09, 2023, from http://tinyurl.com/34zy4jkf

الأسيوطي, أيمن. (2020) الجوانب القانونية لتطبيق الذكاء الاصطناعي. دار مصر للنشر والتوزيع.

حكومة الإمارات العربية المتحدة (2022). تعرف على الذكاء الاصطناعي. Retrieved Nov 09, 2023, from https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

عبد الصادق, عادل (2018). البيانات الشخصية. الصراع على "نفط" القرن الحادي والعشرين. كراسات استراتيجية, *27*(287)https://accronline.com/print_article.aspx?id=29116

عبد المطلب، ممدوح عبد الحميد. (2020) خوارزميات الذكاء الإصطناعي وإنفاذ القانون. دار النهضة العربية.

عيسى, هيثم السيد أحمد. (2019) التشخيص الرقمي لحالة الإنسان في عصر التنقيب في البيانات عبر تقنيات الذكاء الاصطناعي وفقاً للائحة الأوروبية العامة لحماية البيانات لعام *2016*. دار النهضة العربية.

فاضل, علي مولود و عباس, سيف عدنان. (2022). التزييف العميق. لغة الذكاء الاصطناعي في حروب السيبران الإعلامية. دار أمجد للنشر والتوزيع.

فكري, أيمن عبدالله. (2007) جرائم نظم المعلومات. دراسة مقارنة. دار الجامعة الجديدة.

محرم, أحمد مصطفى (2022). استخدامات الذكاء الاصطناعي. استخدام تقنية التزييف العميق في قذف الغير نموذجا. دراسة فقهية مقارنة معاصرة. مجلة البحوث الفقهية والقانونية, *39*(39), 2491-2589. https:// https://doi.org/10.21608/JLR.2022.163670.1114

المناعسة, أسامة أحمد و الزعبي, جلال محمد. (2014) جرائم تقنية نظم المعلومات. دراسة مقارنة (2nd ed.). دار الثقافة للنشر والتوزيع.

الموسوي, واثق علي. (2019) الذكاء الاصطناعي. بين الفلسفة والمفهوم. دار الأيام للنشر والتوزيع.

هارون, محمود طارق. (2019) مدخل إلى علم الذكاء الاصطناعي. الدار الأكاديمية للعلوم.

ثانياً: المراجع الأجنبية:

Al-Business. (2019), *Why deepfakes pose an unprecedented threat to businesses.* Retrieved Nov 09, 2023, from https://aibusiness.com/responsible-ai/why-deepfakes-pose-an-unprecedented-threat-to-businesses

An act to amend the penal law, in relation to unlawful dissemination or publication of intimate images created by digitization and of sexually explicit depictions of an individual; and to repeal certain provisions of such law relating thereto. (2023). https://www.nysenate.gov/legislation/bills/2023/S1042/amendment/A

Bregler, C., Covell, M., & Slaney, M. (2023). Video rewrite: Driving visual speech with audio. *Seminal graphics papers: Pushing the boundaries* (pp. 715-722), https://doi.org/10.1145/3596711.3596787

Brown v. hartlage, 456 U.S. 45 (1982), 1982). https://supreme.justia.com/cases/federal/us/456/45/

Caporusso, N.Deepfakes for the good: A beneficial application of contentious artificial intelligence technology. Paper presented at the *Advances in Artificial Intelligence, Software and Systems Engineering: Proceedings of the AHFE 2020 Virtual Conferences on Software and Systems Engineering, and Artificial Intelligence and Social Computing, July 16-20, 2020, USA,* 235-241. https://doi.org/10.1007/978-3-030-51328-3_33 https://link.springer.com/chapter/10.1007/978-3-030-51328-3_33

Chesney, B., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *Calif.L.Rev., 107*, 1753. https://scholarship.law.bu.edu/faculty_scholarship/640

China Law Translate. (2013, Sep 10,). *Interpretation on several issues regarding the applicable law in cases of using information networks to commit defamation and other such crimes.* https://www.chinalawtranslate.com/en/. Retrieved Feb 29, 2024, from https://www.chinalawtranslate.com/en/spc-and-spp-interpretation-on-internet-speech-crimes/

Chinese Congress. (2020), *Criminal law of the people's republic of china. Chapter IV: Crimes of infringing on citizens' personal rights and democratic rights.* http://en.npc.gov.cn.cdurl.cn/2020-12/26/c_921604_12.htm. Retrieved Feb 29, 2024, from http://en.npc.gov.cn.cdurl.cn/2020-12/26/c_921604_12.htm

Chinese Supreme People's Court. (2022, Dec 08,). *The opinions on regulating and strengthening the applications of artificial intelligence in the judicial fields (2022).* https://www.chinajusticeobserver.com/. Retrieved Feb 29, 2024, from https://tinyurl.com/2sumryek

Chinese Supreme People's Court. (2016, Dec 20,). *Opinions on several issues concerning the application of law in handling criminal cases such as telecommunications network fraud.* https://www.mps.gov.cn/. Retrieved Feb 29, 2024, from https://www.mps.gov.cn/n6557558/c5580478/content.html

Chipman, J., & Preston, S. (2019, Dec 23,). *First federal legislation on deepfakes signed into law.* https://www.wilmerhale.com/. Retrieved Feb 29, 2024, from https://www.wilmerhale.com/insights/client-alerts/20191223-first-federal-legislation-on-deepfakes-signed-into-law

Clough, J. (2015). *Principles of cybercrime* (2nd ed.). Cambridge University Press. https://https://doi.org/10.1017/CBO9781139540803

Coleman, F. (2020). *A human algorithm: How artificial intelligence is redefining who we are*. Melville House UK.

Delfino, R. A. (2019). Pornographic deepfakes: The case for federal criminalization of revenge porn's next tragic act. *Fordham Law Review, 88*(3), 887-932. https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=5640&context=flr

Delfino, R. A. (2023). Deepfakes on trial: A call to expand the trial judge's gatekeeping role to protect legal proceedings from technological fakery. *Hastings Law Journal, 74*(6), 293-348. https://repository.uclawsf.edu/hastings_law_journal/vol74/iss2/3/

Eric hatteberg v. capital one bank USA, N.A. (8:19-cv-01425), 2021). https://www.courtlistener.com/docket/15974713/eric-hatteberg-v-capital-one-bank-usa-na/

Ferraro, M., Chipman, J., & Preston, S. (2020). The federal "Deepfakes" law. *The Journal of Robotics, Artificial Intelligence & Law, 3*(4), 229-233. https://www.wilmerhale.com/-/media/files/shared_content/editorial/publications/documents/20200701-the-federal-deepfakes-law.pdf

Gerstner, E. (2020). Face/off:"DeepFake" face swaps and privacy laws. *Defense Counsel Journal, 87*, 1-14. https://www.iadclaw.org/assets/1/17/Face_Off_-_DeepFake_Face_Swaps_and_Privacy_Laws.pdf?4179; https://heinonline.org/HOL/LandingPage?handle=hein.journals/defcon87&div=4&id=&page=

Ghaemmaghami, & Villafranco, J. (2021). *Deepfake best practices amid developing legal landscape*. Law360.com.

Hallevy, G. (2015). *Liability for crimes involving artificial intelligence systems*. Springer International Publishing. https://https://doi.org/10.1007/978-3-319-10124-8

Hine, E., & Floridi, L. (2022). New deepfake regulations in china are a tool for social stability, but at what cost? *Nature Machine Intelligence, 4*(7), 608-610. https://https://doi.org/10.1038/s42256-022-00513-4

Horowitz, M. C., Allen, G. C., Saravalle, E., Cho, A., Frederick, K., & Scharre, P. (2018). *Artificial intelligence and international security.* (). Washington, DC, USA: Center for a New American Security. https://

www.cnas.org/publications/reports/artificial-intelligence-and-international-security

Kaplan, J. (2016). *Artificial intelligence: What everyone needs to knowR*. Oxford University Press.

Knight, W. (2020, Jun 12,). *Deepfakes aren't very good. nor are the tools to detect them.* Retrieved Nov 09, 2023, from https://www.wired.com/story/deepfakes-not-very-good-nor-tools-detect/

Langa, J. (2021). Deepfakes, real consequences: Crafting legislation to combat threats posed by deepfakes. *Boston University Law Review, 101*, 761-801. https://www.bu.edu/bulawreview/files/2021/04/LANGA.pdf

Lexology. (2021, *Authorship in deepfake movies.* Retrieved Nov 09, 2023, from https://www.lexology.com/library/detail.aspx?g=ef6e81a2-422b-44ee-b640-d536b8080044

Li, X. (2015). Regulation of cyber space: An analysis of chinese law on cyber crime. *International Journal of Cyber Criminology, 9*(2), 185-204. https://https://doi.org/10.5281/zenodo.56225

Liu, H., & Mazibrada, A. (2020). Artificial intelligence affordances: Deep-fakes as exemplars of AI challenges to criminal justice systems. *United Nations Interregional Crime and Justice Research Institute (UNICRI) Special Collection on Artificial Intelligence,* , 59-70. https://unicri.it/sites/default/files/2020-08/Artificial%20Intelligence%20Collection.pdf

Mustak, M., Salminen, J., Mäntymäki, M., Rahman, A., & Dwivedi, Y. K. (2023). Deepfakes: Deceptions, mitigations, and opportunities. *Journal of Business Research, 154*, 113368. https://doi.org/10.1016/j.jbusres.2022.113368

Nguyen, T. T., Nguyen, Q. V. H., Nguyen, D. T., Nguyen, D. T., Huynh-The, T., Nahavandi, S., Nguyen, T. T., Pham, Q., & Nguyen, C. M. (2022). Deep learning for deepfakes creation and detection: A survey. *Computer Vision and Image Understanding, 223*, 103525. https://doi.org/10.1016/j.cviu.2022.103525

Nilsson, N. J. (2009). *The quest for artificial intelligence*. Cambridge University Press.

PEOPLE of the state of michigan, plaintiff-appellee, v. alonte perton SMITH, defendant-appellant, 2021). https://caselaw.findlaw.com/court/mi-court-of-appeals/2112291.html

Ray, A. (2021). Disinformation, deepfakes and democracies: The need for legislative reform. *The UNIVERSITY OF NEW SOUTH WALES LAW JOURNAL, 44*(3), 983-1013. https://https://search.informit.org/doi/10.3316/informit.20211005054413

Reynolds, M. (2020). Courts and lawyers struggle with growing prevalence of deepfakes. *American Bar Association (ABA) Journal-Trials and Litigation,* https://www.abajournal.com/web/article/courts-and-lawyers-struggle-with-growing-prevalence-of-deepfakes

Ridan, X. (2017, *Interpretation of the "interpretation on several issues concerning the application of law in handling criminal cases of infringement of citizens' personal information".* https://www.spp.gov.cn/spp/zdgz/201705/t20170510_190150.shtml. Retrieved Feb 29, 2024, from https://www.spp.

gov.cn/spp/zdgz/201705/t20170510_190150.shtml

Schwartz, O. (2018), *You thought fake news was bad? deep fakes are where truth goes to die.* https://www.theguardian.com/. Retrieved Nov 09, 2023, from https://www.theguardian.com/technology/2018/nov/12/deep-fakes-fake-news-truth

Sheehan, M. (2023). China's AI regulations and how they get made. *Carnegie Endowment for International Peace, 2*, 108-125. https://carnegieendowment.org/2023/07/10/china-s-ai-regulations-and-how-they-get-made-pub-90117

Shin, H., Tenenholtz, N. A., Rogers, J. K., Schwarz, C. G., Senjem, M. L., Gunter, J. L., Andriole, K. P., & Michalski, M.Medical image synthesis for data augmentation and anonymization using generative adversarial networks. Paper presented at the *Simulation and Synthesis in Medical Imaging: Third International Workshop, SASHIMI 2018, Held in Conjunction with MICCAI 2018, Granada, Spain, September 16, 2018, Proceedings 3,* 1-11. https://doi.org/10.1007/978-3-030-00536-8_1 https://arxiv.org/pdf/1807.10225.pdf

Sloot, B., Wagensveld, Y., & Koops, B. (2021). *Deepfakes: The legal challenges of a synthetic society.* (). Netherland: Tilburg University-Tilburg Institute for Law, Technology, and Society. https://repository.wodc.nl/bitstream/handle/20.500.12832/3134/3137-deepfakes-summary.pdf

Tariq, S., Abuadbba, A., & Moore, K.Deepfake in the metaverse: Security implications for virtual gaming, meetings, and offices. Paper presented at the *Proceedings of the 2nd Workshop on Security Implications of Deepfakes and Cheapfakes,* Melbourne, VIC, Australia. 16–19. https://doi.org/10.1145/3595353.3595880 https://arxiv.org/abs/2303.14612

Tashman, A. (2021). "Malicious deepfakes" - how california's A.B. 730 tries (and fails) to address the internet's burgeoning political crisis. *Loyola of Los Angeles Law Review, 54*(4), 1391-1422. https://digitalcommons.lmu.edu/llr/vol54/iss4/8/

The PEOPLE of the state of colorado, plaintiff-appellee, v. daniel J. GONZALES, defendant-appellant, (Colorado Court of Appeals, Division I 2019). https://caselaw.findlaw.com/court/col-crt-app-div-i/1985630.html

Tyagi, K.Deepfakes, copyright and personality rights an inter-disciplinary perspective. Paper presented at the *Law and Economics of the Digital Transformation,* 191-210. https://https://doi.org/10.1007/978-3-031-25059-0_9

van Wyk, B. (2022, Aug 23,). *China's cybercrime problem is growing.* https://thechinaproject.com/2022/08/23/chinas-cyber-crime-problem-is-growing/. Retrieved Nov 09, 2023, from https://thechinaproject.com/2022/08/23/chinas-cyber-crime-problem-is-growing/

Varghese, B. (2023, July 10,). *Deepfakes in texas: What are they and are they illegal?* https://versustexas.com/deepfakes/. Retrieved Feb 29, 2024, from https://versustexas.com/deepfakes/

Vazquez. (2021). *Recommendations for regulation of deepfakes in the U.S.: Deepfake laws should*

protect everyone not only public figures. Epstein Becker Green Law.

Verdoliva, L. (2020). Media forensics and DeepFakes: An overview. *IEEE Journal of Selected Topics in Signal Processing, 14*(5), 910-932. https://https://doi.org/10.48550/arXiv.2001.06564

VMware. (2022, Aug 08,). *VMware report warns of deepfake attacks and cyber extortion.* https://news.vmware.com/emea. Retrieved Nov 09, 2023, from https://news.vmware.com/releases/vmware-report-warns-of-deepfake-attacks-and-cyber-extortion

Wang, Q. (2016). *A comparative study of cybercrime in criminal law: China, US, england, singapore and the council of europe* (PhD). hdl.handle.net/1765/94604

Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review, 9*(11), 39-52. https://timreview.ca/article/1282

Yang, F., & Feng, J. (2021). Rules of electronic data in criminal cases in china. *International Journal of Law, Crime and Justice, 64*, 1-11. https://doi.org/10.1016/j.ijlcj.2020.100453

Yasrab, R., Jiang, W., & Riaz, A. (2021). Fighting deepfakes using body language analysis. *Forecasting, 3*(2), 303-321. https://doi.org/10.3390/forecast3020020

Yong, P. (2011, *Comparative research on "convention on cybercrime" and chinese relevant legislation.* https://www.coe.int/en/web/portal/home. Retrieved Nov 09, 2023, from https://www.coe.int/t/dg1/legalcooperation/economiccrime/cybercrime/Documents/CountryProfiles/567%20china-d-Comparative%20Research_ed1a.PDF

Zhang, L. (2019). *Initiatives to counter fake news in selected countries. china.* The Law Library of Congress. https://tile.loc.gov/storage-services/service/ll/llglrd/2019668145/2019668145.pdf

الترجمة الصوتية لمصادر ومراجع اللغة العربية: Romanized Arabic References:

ʾibrāhym- sārata (2021) ،kayfa tughayyiru ʿamaliyyātu al-tzyīfi almutqinati naẓratanā lil-wāqiʿi https://www.swissinfo.ch/ara/. Retrieved Nov 09, 2023, from http://tinyurl.com/34zy4jkf

al-ʾāsyūṭiyyu- ʾaymanu (2020) aljawānibu alqānawniyyatu litaṭbīqi al-dhakāʾi aliāṣṭināʿiyyi dār miṣra lil-nashri wa-l-tawzīʿi

ḥukūmatu al-ʾimārāt al-ʿrbya al-mtḥda (2022). tʿrf ʿalā al-dhkāʾ al-aṣṭināʿiyyi Retrieved Nov 09, 2023, from https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence

ʿabdu al-ṣādiqi- ʿādilun (2018). albayānātu al-shakhṣiyyatu al-ṣirāʿu ʿalā" nifṭi " alqarni alḥādī wa-l-ʿishrīna kurrāsātun astirātiyyajy#- 27(287) https://accronline.com/print_article.aspx?id=29116

ʿabdu almuṭṭalibi mamdūḥun ʿabdu alḥamīdi (2020) khūārizmiyyātu al-dhakāʾi alʾiṣṭināʿiyyi waʾinfādhu alqānūni dāru al-nahḍati alʿarabiyyati

ʿīsā- haythamu al-sayyidi ʾaḥmd (2019) al-tashkhīṣu al-raqmiyyu liḥālati alʾinsāni fī ʿaṣri al-tanqībi fī albayānāti ʿabra tiqniyyāti al-dhakāʾi aliāṣṭināʿiyyi wafqan lil-āʾiaḥati al-ʾāūrūbbiyyati alʿāmmati liḥimāyati albayānāti liʿāmi 2016. dāru al-nahḍati alʿarabiyyati

fāḍil- ʿaliyyun mawlūdun w ʿabbās- sayfu ʿadnāna (2022). al-tazyīfu alʿamīqu lughatu al-dhakāʾi aliāṣṭināʿiyyi fī ḥurūbi al-saybrān alʾiʿlāmiyyati. dāru ʾamjd lil-nashri wa-l-tawzīʿi

fikriyy- ʾaymanu ʿibdālilh (2007) jarāʾimu naẓmi almaʿlūmāti dirāsatun muqārinatun dāru aljāmiʿati aljadīdati

mḥrm- ʾaḥmd muṣṭafā (2022). istakhdāmiāt al-dhakāʾi al-aṣṭināʿiyyi astikhdāmu tiqniyyati al-tzyīfi alʿamīqi fī qadhfi alghayri nmwdhjā dirāsatun fiqhiyyatun muqārinatun muʿāṣiratun mjla albuḥūthi alfiqhiyyati wa-l-qqianwinnayi#- 39(39), 2491-2589. https://https://doi.org/10.21608/JLR.2022.163670.1114

almunāʿasa#u- usāmatu ʾaḥmadu w al-zaʿbiyyu- jalāl muḥammadin (2014) jarāʾimu tiqniyyati naẓmi almaʿlūmāti dirāsatun muqārinatun (2nd ed.). dāru al-thaqāfati lil-nashri wa-l-tawzīʿi

almawsuī- wāthiq ʿly (2019) al-dhakāʾu aliāṣṭināʿiyyu bayna alfalsafati wa-l-mafhūmi dār al-ʾāyyāmi lil-nashri wa-l-tawzīʿi

hārūnu- maḥmūd ṭāriqin (2019) madkhalun ʾilā ʿilmi al-dhakāʾi aliāṣṭināʿiyyi. al-dāru al-ʾākāadyimmayu lil-ʿulūmi

Penal Response to Digital Content Manipulation Using Deepfake Technology in Chinese Legislation: A Comparative Descriptive Study

Muaath Suleiman AL-Mulla(1)

Abstract:

Recently, methods of digital content manipulation have evolved through applications referred to by the Chinese regulator as "Deep Synthesis", thanks to artificial intelligence technology (AI) that has enhanced content quality. The significance of this research lies in its discussion of a relatively recent topic that has emerged due to the misuse of these applications. The problem lies in deploying these technologies for illicit purposes, until the new term "Deepfake" emerged to express the possibility of tampering with digital content in a way close to real content. This is further compounded by the loss of ethical controls in the rapid production and development of these technologies. This research aims to explain the nature of digital content manipulation using deep synthesis technologies and applications, the dangerous impact of the misuse of Deepfake on societies' security in the cyber environment, as well as the extent to which that manipulation is considered a criminal offense subject to the concept of cybercrimes. The research also examines how China, as one of the first countries to establish regulations to mitigate the risks of misuse of these technologies, has addressed this issue, including the penalties imposed and the position of comparative criminal laws. To achieve its objective, the study adopted the descriptive and comparative approaches, concluding with results and recommendations that ensure an effective response to the misuse of Deep synthesis applications.

Keywords: Deep synthesis, Deepfakes, Misuse, Cybercrime, Artificial intelligence, Criminal law, Chinese regulator.

(1) Kuwait International Law School (Kuwait City – Kuwait)
m.almulla@kilaw.edu.kw