المخاطر الأمنية والمجتمعية للتزييف العميق وآليات المواجهة

د. سامح محمد محمد السيد إبراهيم

عضو هيئة التدريس- جامعة نايف العربية للعلوم الأمنية

(ISSN: 2537- 0758)

المخاطر الأمنية والمجتمعية للتزييف العميق وآليات المواجهة

د. سامح محمد محمد السيد إبراهيم

الملخص:

التزييف العميق (Deepfake) يُعتبر واحدًا من أخطر التطورات التكنولوجية في العصر الرقمي، حيث تُستخدم تقنيات الذكاء الاصطناعي التوليدية لإنشاء محتوى رقمي مزيف يتمتع بدرجة عالية من الواقعية، سواء كان ذلك فيديوهات أو صورًا أو أصواتًا. هذه التقنية تُشكل تهديدًا كبيرًا على مستويات متعددة، بدءًا من انتهاك الخصوصية الشخصية ووصولًا إلى تهديد الأمن القومي. يُمكن استخدام التزييف العميق لنشر الأخبار الكاذبة، التلاعب بالرأي العام، التشهير بالأفراد، وحتى تنفيذ عمليات احتيال متطورة عن طريق تقليد أصوات أو وجوه شخصيات موثوقة. بالإضافة إلى ذلك، تُساهم هذه التقنية في تآكل الثقة بالمعلومات الرقمية، مما يُعقد جهود التحقيق الجنائي ويزيد من مخاطر الجرائم السيبرانية.

لقد أصبح التزييف العميق أداة قوية في يد الجهات الخبيثة، حيث يُستخدم لابتزاز الأفراد ماليًا أو جنسيًا، أو لنشر الشائعات والمعلومات المضللة بسرعة كبيرة، مما يُسبب أضرارًا نفسية واجتماعية جسيمة للضحايا. كما أن هذه التقنية تُستخدم في عمليات الاحتيال المتطورة، حيث يتم تقليد أصوات ووجوه الشخصيات الموثوقة لخداع الضحايا والحصول على معلومات حساسة أو تنفيذ معاملات مالية غير مشروعة.

لذلك، أصبح من الضروري مواجهة هذه التهديدات من خلال تطوير أدوات متقدمة للكشف عن المحتوى المزيف، حيث يجب على الشركات التقنية والحكومات الاستثمار في بحوث الذكاء الاصطناعي لتطوير أنظمة قادرة على تمييز المحتوى الحقيقي من المزيف. بالإضافة إلى ذلك، يجب سن تشريعات صارمة تجرم استخدام التزييف العميق في الأنشطة غير القانونية، مع فرض عقوبات رادعة على المخالفين.

ومن ناحية أخرى، يجب تعزيز الوعي المجتمعي بمخاطر هذه التقنية، حيث يحتاج الأفراد إلى فهم كيفية حماية أنفسهم من خلال توخي الحذر عند مشاركة الصور أو الفيديوهات الشخصية على الإنترنت. كما يجب على المؤسسات تعزيز إجراءاتها الأمنية لمواجهة التهديدات الناشئة عن التزييف العميق، بما في ذلك استخدام تقنيات التحقق من الهوية المتقدمة.

أخيـرًا، يُعد التعـاون الـدولي أمـرًا بـالغ الأهميـة فـي مكافحـة التزييـف العميـق، حيـث يتطلب الأمر تبادل الخبرات والتقنيات بين الدول لضمان حماية الأفراد والمجتمعات من تـأثيرات هـذه الظـاهرة الخطيـرة. فقـط مـن خـلال الجهـود المشـتركة بـين الحكومـات والمؤسسات التقنية والمجتمع المدني يمكننا الحد من مخاطر التزييف العميق وضمان استخدام التكنولوجيا بشكل أخلاقي وآمن.

The security and societal risks of deepfakes and coping mechanisms

Abstract:

Deepfake is considered one of the most dangerous technological developments in the digital age, where generative artificial intelligence (AI) technologies are used to create highly realistic fake digital content, including videos, images, and audio. This technology poses a significant threat on multiple levels, ranging from personal privacy violations to national security risks. Deepfakes can be used to spread fake news, manipulate public opinion, defame individuals, and even carry out sophisticated fraud by mimicking the voices or faces of trusted figures. Additionally, this technology contributes to the erosion of trust in digital information, complicating criminal investigations and increasing the risks of cybercrime.

Deepfake has become a powerful tool in the hands of malicious actors, used for financial or sexual extortion, or to rapidly spread rumors and misinformation, causing severe psychological and social harm to victims. This technology is also employed in advanced fraud schemes, where the voices and faces of trusted individuals are replicated to deceive victims into revealing sensitive information or conducting unauthorized financial transactions.

Therefore, it is essential to address these threats by developing advanced tools to detect fake content. Tech companies and governments must invest in AI research to create systems capable of distinguishing real content from fake.

(ISSN: 2537- 0758)

Additionally, strict legislation must be enacted to criminalize the use of deepfakes in illegal activities, with deterrent penalties for violators.

On the other hand, public awareness of the risks of this technology must be heightened. Individuals need to understand how to protect themselves by being cautious when sharing personal photos or videos online. Institutions must also enhance their security measures to counter emerging threats from deepfakes, including the use of advanced identity verification technologies.

Finally, international cooperation is crucial in combating deepfakes. It requires the exchange of expertise and technologies between nations to ensure the protection of individuals and societies from the harmful effects of this dangerous phenomenon. Only through joint efforts by governments, tech companies, and civil society can we mitigate the risks of deepfakes and ensure the ethical and safe use of technology.

أولاً- مقدمة

انتشر في الفترة الأخيرة كثير من مقاطع الفيديو المفبركة التي تخص أشخاصاً مشاهير أو سياسيين، وكانت هذه المقاطع تبدو حقيقية وعصيَّة على التكذيب لدرجة أنَّها تسببت بفضائح أخلاقية لهم، لكن بعد التدقيق والتمحيص تم التوصل إلى زيف هذه المشاهد، واكتشاف الطريقة التي صُمِمَت بها، بكل هذه الاحترافية والإتقان، فكانت تقنية التزييف العميق الـ "ديب فيك" (Deep fake)، وفي عالم اليوم الذي يمتلئ بمنصات التواصل الاجتماعي والمواقع والصفحات والتطبيقات الإلكترونية المتنوعة، يمكن يزداد احتمال وقوع الأشخاص ضحية لتضليل أو استقطاب خاصة عندما يتم دمج مقطع فيديو مزيف إلى سلسلة من الأكاذيب أو الأخبار الوهمية، وتعتبر تقنية التزييف العميق Deepfake أحد أنواع تطبيقات الذكاء الاصطناعي AI، والتي تتيح إنتاج مقاطع ووسائط مرئية وصور اصطناعية، بحيث يُخيَّل لمن يشاهدها أول مرة كأنها حقيقية

بالفعل[١].

ويمكن لهذا التضليل أو التلاعب التأثير على الرأي العام من خلال استهداف شخصيات سياسية بإنشاء لقطات مزيفة لهم وهم يقولون أشياء لم ترد على ألسنتهم، أو يرتكبون أفعالا لم يتم اقترافها من قبل، ومن مساوء التزييف "القصف والتشهير بالمشاهير والقادة وأصحاب الشركات والمرشحين للرئاسة والشخصيات الدينية وقادة الفكر والثقافة وغيرهم" باستخدام تقنية التزييف العميق على مدار السنوات القادمة، في حين سيقع على عاتق المواطن العادي أن يميز بنفسه بين ما هو حقيقي أو مزيف[٢].

وشهدت السنوات الأخيرة ارتفاعًا كبيرًا في عدد محتوى التزييف العميق عبر الإنترنت، حيث ارتفع بنسبة ٩٠٠% بين عامي ٢٠١٩ و٢٠٢٠. وتظهر التوقعات أن هذا الاتجاه المقلق سيستمر في السنوات القادمة، ومن المتوقع أن يصل "ما يصل إلى ٩٠% من المحتوى عبر الإنترنت" إلى أن يتم إنشاؤه صناعيًا بحلول عام ٢٠٢٦، وفقًا لبعض الباحثين[٣].

ثانيًا- مشكلة البحث:

مع تزايد خطر الجرائم المستحدثة ومنها **التزييف العميق** وتنامي المنصات الإلكترونية التي اعتمدت في الآونة الأخيرة على شبكة المعلومات الدولية كوسيلة لها قدرة كبيرة على التأثير على كل فئات المجتمع من خلال مواقعها المختلفة (كالفيسبوك وتويتر ويوتيوب وغيرها من المواقع التي تستخدمها شريحه عريضة من فئات المجتمع وخاصة الشباب، ومن هنا يظهر لنا أن المشكلة التي تدور حولها الدراسة هي توضيح الدور الذي تلعبه برامج التزييف العميق والتلاعب بالبيانات والأرقام والصور والفديوهات عبر مواقع التواصل الاجتماعي في صناعة وتطور الجرائم وانتهاك حقوق الإنسان

---

(1) X. Yang, Y. Li and S. Lyu, "Exposing Deep Fakes Using Inconsistent Head Poses," ICASSP 2019- 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2019, pp. 8261-8265

(2) Tu, C.Z.; Yuan, Y.; Archer, N.; Connelly, C.E. Strategic value alignment for information security management: A critical success factor analysis. Inf. Comput. Secur. 2018, 26, 150–170. www.scopus.com

(٣) المنتدى الاقتصادي العالمي دافوس٢٠٢٣ المقام في دولة سويسرا التقرير متاح علي:
https://www.swissinfo.ch/ara

(ISSN: 2537- 0758)

والخصوصية واستغلال الفضاء الإلكتروني في تنفيذ تلك الجرائم المستحدثة.

ثالثًا- أهمية الدراسة:

أصبحت صناعة الفديوهات المزيفة لها اضرار سياسية اجتماعية وامنية هائلة في ضوء التقدم التقني السريع والإنتشار السريع للمنصات المختلفة الجنسيات والأعراق موضوعاً في غاية الأهمية، لكي نضع خطوط دفاع تكنولوجية لمواجهة دواعي **مخاطر التزييف العميق** عبر البيئة السيبرانية، والعديد من دول العالم تركز على كيف توظف الذكاء الاصطناعي بالشكل الذي يرفع من فاعلية حصر البيانات المطلوبة وتوظيفها لخدمة اهدافها الرئيسية وخاصة الأمنية ومكافحة الإرهاب **ومواجهة التطرف العنيف والأزمات السياسية**" عبر منصات التواصل الاجتماعى التي تنتشر بقوة عالميا، **وتدشين شراكة قوية بين شركات التكنولوجيا والأجهزة الأمنية.**

رابعًا- أهداف الدراسة

- التعرف على تقنية التزييف العميق وكيف تعمل وتحديد مخاطرها السياسية والإجتماعية والأمنية والى أي مدة تأثيره على المجتمعات ومعرفة أنواعة (الفديو– الصوت– الصور) المزيفة مع أهمية المحافظة عليها من المخاطر المحيطة، مع التعرف على أنماط الصراع في عصر المعلومات.
- **التعرف على أهم تطبيقات التوصل الاجتماعى استخداماً للتزييف العميق** واعداد مستخدمي المنصات في الدول العربية ومدى خطورة التطبيقات على مستوي الأمن القومي والعربي
- الى أي مدى تقع خطورة جرائم التزييف العميق كأحد جرائم تقنيات المعلومات وخاصة غسيل العقول ونشر الشائعات والأخبار المزيفة وأشكال التزييف والأخطر وهو التحريض على والعنف في منصات التواصل الاجتماعي.
- تهدف هذه الدراسة بشكل عام للتعرف على مراحل ومكونات الذكاء الاصطناعي التي تستخدم في عملية رصد التزييف العميق والخلايا العصبية المكونة له والمقصود بالهندسة العكسية ودور تعلم الآلة والخوارزميات ومعالجة اللغات الطبيعية والشبكات العصبية الذكية لقدرة الأنظمة على الوصول لأكتشاف فديوهات وصور ومقطوعات صوتية مزيفة.

خامساً- تساؤلات الدراسة:

- **ما هو تعريف التزييف العميق وآلياته وكيفية استخدامه؟**
- ماهي الأليات المستحدثة لمواجهة التزييف العميق وما هي مخاطرة الأمنية والمجتمعية ومدى تأثيرها على المجتمع وما هي قدرة الذكاء الاصطناعى على اكتشاف التزييف العميق؟
- ما هي مواقع التواصل الاجتماعى المستخدمة عربياً وأسباب زيادة نسب اعداد مستخدمي منصات التواصل الاجتماعى بتلك المنصات ومدى خطورتها؟
- ما هي المخاطر المرتبطة بالتزييف العميق والأشكال الأخرى للمحتوى الذي يتم إنشاؤه بواسطة الذكاء الاصطناعي، وما هي المخاطر الأمنية لتطبيقات التزييف العميق والمؤثرة على الأمن القومي والعربي– وما هي أخطار على المستوي الامني والسياسي وعلاقة التطبيق بنشر العنف وثقافته؟

سادساً- منهج البحث:

فرض الموضوع محل الدِراسة "المخاطر السياسية للتزييف العميق وآليات المواجهة"، الذي يهدف لتحديد أليات مستحدثة لمواجهة التزييف العميق عبر المنصات الإلكترونية بسبب تطور معدلات استخدام الإنترنت ومواقع التواصل الاجتماعى الأمر الذي يدل على سرعة انتشار الأخبار الكاذبة والفيديوهات المزيفة بين المستخدمين، وبيان الآثار المترتبة عليها، مع ضرورة الاعتماد على المنهج الوصفى التحليلى؛ حيث توضح المُقدمات وتأصيلها، واستعراض التقنيات الداعمة لكشف التزييف العميق.

سابعاً- مصطلحات الدراسة:

التزييف العميق Deepfake**– الذكاء الاصطناعي– الشبكات العصبية– التعلم الآلي والعميق– الخوارزميات–منصات التواصل الاجتماعي– نظام GAN.**

ثامناً- خطة الدراسة:

بداية جاء المبحث الأول، التنزيف العميق ومخاطرة، ويضم مطلبين، الأول ماهية وأنواع التنزيف العميق، والثاني المخاطر الأمنية والاجتماعية للتزييف العميق وأشكال الخداع، **وجاء المبحث الثاني** آليات مواجهة التزييف العميق، واشتمل مطلبين، الأول المواجهة القانونية لجرائم التزييف العميق، والثاني الآليات التقنية والأمنية لمواجهة التزييف العميق، **ثم الخاتمة وأهم النتائج والتوصيات.**

(ISSN: 2537- 0758)

المبحث الأول
التنزيف العميق ومخاطرة

في الماضي القريب، كان السبيل الوحيد للتزييف برنامج معالجة الصور (فوتوشوب)، والذي كان يستخدم حصرًا من قبل المصممين المحترفين بتعديل وتركيب الصور، أما **التزييف العميق deepfakes** فيتخذ منحى من مناحي الذكاء الاصطناعي، والذي يسمى التعلم العميق Deep Learning لإنتاج صور وفيديوهات لأحداث مزيفة[٤] ويخشى الكثيرون من أن التكنولوجيا ستزيد بشكل كبير من **تهديد المعلومات** المضللة الأجنبية والمحلية، **وكان لذا التهديد أثر واضح للعديد من النساء اللواتي استهدفتهن المواقع الإباحية التي تدعم الذكاء الاصطناعي**[٥].

والتزييف العميق يستخدم كوسيلة للابتزاز حيث تؤدي التطورات التكنولوجية والتحسين النوعي في مجال الذكاء الاصطناعي والتعلم العميق إلى إنشاء محتوى رقمي واقعي المظهر، ولكنه زائف يعرف باسم التزييف العميق يمكن مشاركة مقاطع الفيديو التي تم التلاعب بها بسرعة عبر وسائل التواصل الاجتماعي لنشر أخبار مزيفة أو معلومات مضللة لا تؤثر فقط على أولئك الذين يتم خداعهم وتؤثر على المجتمعات[٦].

في عام ٢٠٢٢، شهدنا زيادة كبيرة في هجمات التزييف العميق داخل المؤسسات وتأثر حوالي ٦٦% من المحترفين والموظفين المسؤولين عن الأمن السيبراني بهذه الهجمات. وتعتبر إنشاء رسائل صوتية مزيفة واحدة من أمثلة جرائم التزييف العميق

---

[٤] هشام الزوام، تقنية التزييف العميق بين الفوائد والأضرار.. وطرق الاكتشاف، بوابة الاقتصاد الرقمي الأولي، بتاريخ ، ١١ يناير ، ٢٠٢٢ ومتاح على:
https://followict.news/

[٥] عمار ياسر البابلي، المخاطر الأمنية للتزييف العميق وآليات المواجهة، مجلة الفكر الشرطي، مركز بحوث شرطة الشارقة بالإمارات العربية المتحدة عدد اكتوبر– العدد ١٢٧– أكتوبر ٢٠٢٣، ص ٥٩.

[٦] سماح بن ابراهيم، استخدام تقنية الذكاء الاصطناعي (التزييف العميق) في الفبركة الإعلامية دراسة تحليلية لعينة من الفيديوهات المنشورة على منصة تويتر الانتخابات الرئاسية الأمريكية لسنة ٢٠٢٠ نموذجا، رسالة ماجستير، جامعة قاصدي مرباح، الجزائر، ٢٠٢٠، ص٣٠٨.

التي انتشرت بشكل كبير. تستخدم هذه الهجمات برامج تعديل الصوت وتقنيات أخرى لتحريف أصوات أشخاص معروفين، مما يُجعل الرسائل الصوتية المُزيَّفة تبدو وكأنها مصدرها شخص ذو مصداقية(٧).

وأظهرت الأبحاث أن القطاع المصرفي يعاني من قلق بالغ بسبب هجمات التزييف العميق، حيث يشعر ٩٢% من الممارسين والمتخصصين في الأمن السيبراني بالقلق من إساءة استخدام التزييف العميق للأغراض الاحتيالية. وتشير التقديرات إلى أن ٢٦% من الشركات الصغرى و٣٨% من الشركات الكبيرة تعرضت للاحتيال المزيف العميق؛ مما أدى إلى خسائر تصل إلى ٤٨٠ ألف دولار أمريكي، **ونتناول هذا المبحث كالتالي:**

المطلب الأول
ماهية وأنواع التنزيف العميق

تقوم تقنية التزييف العميق على صنع فيديوهات آخر، عبر برامج الكمبيوتر من خلال الذكاء الاصطناعي، وتعمل هذه التقنية على **محاولة دمج** عدد من الصور ومقاطع الفيديو لشخصية ما بمساعدة تقنية التعلّم الآلي(٨)، من أجل إنتاج مقطع فيديو جديد قد يبدو أنّه حقيقياً، لكنه في واقع الأمر مزيف، وهو لقطات معدلة صناعيا تم فيها تعديل الوجه أو الجسم المصور رقميا ليظهر كشخص أو أي شيء آخر، **وفي المقابل**، تستطيع هذه التقنية الجديدة أيضاً العمل بطريقة عكسية، وتحويل الفيديو إلى صور ورسوم(٩)، **ونتناول ماهية وأنواع التنزيف العميق كالتالى:**

---

(٧) تقرير الذكاء الاصطناعي ومخاطر التزييف العميق، توجهات عالمية، مركز المعلومات واتخاذ القرار، رئاسة مجلس الوزراء المصري، بتاريخ ٢٥ مايو ٢٠٢٣ ومتاح على:
https://www.idsc.gov.eg/DocumentLibrary/LandingPage

(٨) أحمد عبد الموجود أبوالحمد زكير، جريمة التزييف الإباحي العميق (دراسة مقارنة)، المجلة القانونية (مجلة متخصصة في الدراسات والبحوث القانونية) مجلة علمية محكمة، جامعة قانون الوادي، ٢٠٢٢، ص ٢٢٢٧.

(٩) احمد مصطفى معوض، استخدام الذكاء الاصطناعي–تقنية التزييف العميق deep fake في قذف الغير نموذجا دراسة فقهية مقارنة معاصرة، مجلة البحوث الفقهية والقانونية، جامعة الأزهر، العدد ٣٩، أكتوبر ٢٠٢٢، ص ٣٥.

(ISSN: 2537- 0758)

أولاً- تعريف التزييف العميق Deepfake:

الـ Deepfake أو التزييف العميق هي تقنية تستخدم في تزييف مقاطع الفيديو بصورة يصعب على البشر تمييزها والتفرقة بين ما هو حقيقي وبين ما هو مزيف، تعود تسمية الـ Deepfake إلى مصطلح الـ AI Deep Learning Algorithm وهو ما يعني بالعربية خوارزميات التعلم العميق للذكاء الاصطناعي، وهذه الخوارزميات تتميز بأنها قادرة على حل أي مشكلة عندما نزودها بقدر مهول من البيانات عن الأمر(١٠).

و"**تقنية Deepfake**": هي تلك التكنولوجيا التي تستخدم منهجية التعلم العميق Deep learning، التي تُعتبر أحد مكونات الذكاء الاصطناعي، بهدف عمل **محاكاة غير حقيقية** لموقف أو شخص تبدو وكأنها حقيقية ولكنها ليست كذلك على الإطلاق، ويأتي مصطلح deep من فكرة التعلم، وfake من فكرة الخداع والتزوير، ومصطلح "**التزييف العميق**" عملية جمع ملفات الصوت والفيديو بواسطة الذكاء الاصطناعي أو التعلم الآلي بشكل دقيق، وتكون كافة مجالات "التزييف العميق" ممكنة بداية من تبديل الوجوه بمعنى استبدال وجه شخص بآخر أو تزامن تحريك الشفاه إذ يمكن ضبط فم المتحدث على ملف صوتي مختلف عن الصوت الأصلي أو استنساخ الصوت.

ويتم استنساخ نسخة من الصوت من أجل استخدامها لقول أشياء أخرى(١١).

وتستخدم حالياً تقنية التزييف العميق في إنشاء مقاطع فيديو تم استبدال فيها أوجه الأشخاص الحقيقيين بآخرين أو في إنشاء مقاطع فيديو يقول فيها سياسيون ومشاهير كلمات لم ينطقوا بها قط.

---

(10) Eling, M.; Wirfs, J. What are the actual costs of cyber risk events? Eur. J. Oper. Res. 2019, 272, 1109–1119. www.scopus.com

(11) Dayani, Raveena ،Nikita Chhabra, Tarina Kadina, and Rishabh Kaushal. (2015). "Rumor Detection in Twitter: An Analysis in Retrospect." In 2015 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS) 1–3.

ويشير المصطلح إلى برمجية معينة اكتسبت شهرة على Reddit، بإمكانها زرع وجه شخص في مقطع فيديو يظهر فيه شخص آخر، وقد استُخدمت في إنشاء مواد إباحية ونشرها بغرض الإساءة إلى بعض المشاهير. ووفقًا لبعض التقديرات، فإن ٩٦% من جميع محتوى التزييف العميق هو مواد إباحية، ما يسلّط الضوء على المخاوف من استخدام هذه التقنية فى الإساءة والابتزاز والتشهير[١٢].

ثانياً- كيف تعمل تقنية ال Deepfake:

يشار إلى أن التزييف العميق تقنية تعتمد على الذكاء الاصطناعي الذي يستبدل صورة وجه أو صوت أو كليهما بوجه وصوت شخص آخر لتبدو الوسائط المرئية والسمعية المزيفة كأنها حقيقة[١٣]، وعلى الرغم من أنها تقنية مستخدمة في صناعة الدراما السينمائية، إلا أن الثورة الحادثة في التكنولوجيا الرقمية مكنت أفراداً عاديين من استخدام هذه التقنية، وبينهم من يستغلها في تصرفات غير سوية تلحق الضرر بالأفراد والمجتمعات. وتحظى السياسة بنصيب كبير من التحريض والتنمر والتحرش والابتزاز والنصب والاحتيال، وسبق وتم استعمال تقنية التزييف العميق لتزييف خطب وهمية يلقيها زعماء ومحادثات غير حقيقية تدور بين كباء المسؤولين وتسريبات لم تحدث غيّرت مجرى أحداث في دول وشعوبها.

ومن ثم يمكن القول بأن التزييف العميق عبارة عن نسخة متطرفة ملفقة وهمية من بيانات سمعية وبصرية تم التلاعب بها من خلال أحد تطبيقات الذكاء الإصطناعي المعدة لذلك والذي يعني في جوهره التقول علي شخص بشي لم يقله بواسطة تقنيات تكنولوجية حديثة وبحسب البرلمان الاوروبي فالتزييف العميق له مدلول أوسع من الوسائط الحوسبية المركبة التي تقف عند حد تعديل أو تنميط

---

[١٢] تقرير شركة كاسبرسكي المتخصصة في أمن وسلامة المعلومات عن مخاطر الأمن والخصوصية ذات الصلة بالواقع المعزز والواقع الافتراضي، متاح على موقع كاسبرسكي:
https://me.kaspersky.com/resource-center/threats/security-and-privacy-risks-of-ar-and-vr

[١٣] مصطفى صلاح عبدالحميد، التزييف الرقمي وأثره على حجية الأدلة الرقمية في الدعاوي الجنائية دراسة فقهية مقارنة، مجلة الفقه المقارن، كلية الشريعة القانون، جامعة الأزهر، القاهرة، المقالة ١٤، المجلد ٤٠، العدد ٤٠، أكتوبر ٢٠٢٢، ص ٨١١.

(ISSN: 2537- 0758)

البيانات الاصلية اذ يستهدف توليد وتقليد صوت أو صورة أو فيديو بواسطة الذكاء الاصطناعي لا علاقة له بحقيقة الواقع من خلال إستنساخ الصوت أو تحريف الصورة أو تركيب النص(١٤).

وتعمل تقنية التزييف العميق من خلال التعلم الآلي عبر تغذيتها بعدد كبير جدًّا من الصور ومقاطع الفيديو والأصوات ومن خلال الخلايا العصبية الشبكية تقوم هذه النظم عبر خوارزميات ذكية بفبركة وجوه وأشخاص وأصوات غير حقيقية، أو عمل محاكاة لهم تبدو وكأنها واقعية، لكنها غير حقيقية على الإطلاق، ويحدث ذلك من خلال قيام نظام التعلم العميق Deep Learning بدراسة الشخصية المرجو محاكاتها أو تزويرها(١٥)، وذلك عبر استخدام كميات كبيرة من الصور والفيديوهات التي تحاكي كافة زوايا الشخصية المطلوبة- فمثلًا يتم دراسة طريقة هذه الشخصية في الحديث من حركات الوجه والفم والعينين وحركات الأيدي والحركات اللاإرادية التي تقوم بها هذه الشخصية، ثم محاكاة نبرة الصوت الخاصة بها عبر استخدام كميات كبيرة من تسجيلاتها الصوتية، ومن ثم يقوم نظام الذكاء الاصطناعي بفبركة حديث كامل لهذه الشخصية لم تقم به من قبل على الإطلاق(١٦).

ثالثاً- تزايد نسب مستخدمى الإنترنت ومواقع التواصل الإجتماعى عربياً:

تزداد معدلات مستخدمي الإنترنت حول العالم "**٤.٧ مليار مستخدم" طبقاً لإحصائيات في يناير ٢٠٢٥**(١٧)، لذا يلزم الإهتمام بالأمن السيبراني والحفاظ علي

---

(١٤) محمود سلامة عبدالمنعم الشريف، جريمة الانتقام الإباحي عبر تقنية التزييف العميق" Deepfakes" والمسؤولية الجنائية عنها، مجلة كلية الحقوق، جامعة الإسكندرية، المقالة ٥، المجلد ٢.٢٠٢٢، العدد ١، يوليو ٢٠٢٢،ص ص ٤٨٥-٣٦٦.

(١٥) أحمد حازم مصطفي، مقال "تقنية المعلومات"، حكومة دبي، هيئة المعرفة والتنمية البشرية، ٢٠١٥، ص١٨.

(١٦) سامح محمد الشريف، تحليل البيانات الضخمة في تحليل مواقع التواصل الاجتماعي، مجلة رؤي استراتيجية، علمية محكمة، المجلد السابع، العدد (١٩)، يونيو ٢٠٢٠، ص١١-١٨.

(17) DIGITAL 2021: GLOBAL OVERVIEW REPORT ON: https://datareportal.com/

سرية المعلومات باعتبارها قضية أمن قومي، **ويوضح الجدول التالي اعداد مستخدمي مواقع التواصل الاجتماعي بين دول المنطقة العربية في الربع الأخير من عام ٢٠٢٤**[١٨]:

ويُعد فيسبوك (أكثر من ٣ مليار مستخدم) من أبرز المنصات لنشر الفيديوهات والمنشورات التفاعلية، بينما يُستخدم تويتر (٤٥٠ مليون مستخدم) لنشر المعلومات والمنشورات بسرعة عبر الهاشتاقات، مما يسمح بانتشار المعلومات بشكل فوري وواسع[١٩].

من ناحية أخرى، يُعتبر إنستغرام (٢ مليار مستخدم) منصة مثالية للوصول إلى فئة الشباب عبر المحتوى المرئي الجذاب مثل الصور والفيديوهات القصيرة (الريلس)، أما يوتيوب (٢.٥ مليار مستخدم) فيُستخدم لنشر فيديوهات تعليمية طويلة[٢٠] وبرنامج واتساب (٢ مليار مستخدم) لإرسال رسائل شخصية مباشرة إلى الأفراد والمجموعات بالإضافة تيليغرام (٨٠٠ مليون مستخدم).

بالإضافة إلى هذه المنصات، تُستخدم تيك توك (١.٥ مليار مستخدم) حيث يقوم بنشر محتويات صغيرة لكن تنتشر بسرعة عالية تحتوي على الفيديوهات القصيرة، مما يجذب اهتمام الشباب.

رابعاً- تصنيف المحتوى المُزيَّف:

والجدير بالذكر: أن هذه التقنية تعتبر من الأساليب السهلة والبسيطة للتعديل على الفيديوهات أو تركيبها بالكامل، مما يجعلها خطيرة وتفتح باب لإساءة سمعة

(18) GLOBAL SOCIAL MEDIA STATISTICS: https://datareportal.com/social-media-users#:~:text=Furthermore%2C%2017%20social%20media%20platforms,advertising%20reach%20is%202.515%20billion&text=WhatsApp%20has%20at%20least%202%20billion%20monthly%20active%20users

(19) https://datareportal.com/reports/digital-2025-sub-section-ever-more-connected

(20) Digital 2025: AI accelerates, YouTube tops user charts, social ad spend soars and more:
Report finds that internet users have passed the 5.5 billion mark, with 136 million new users added in the last 12 months AT:
https://finance.yahoo.com/news/digital-2025-ai-accelerates-youtube-050000966.html

(ISSN: 2537- 0758)

الآخرين أو الترويج لأجندة معينة، واعتمدت خوارزميات التزييف العميق على إنشاء صور ومقاطع فيديو مزيفة لا يستطيع البشر تمييزها عن الصور الأصلية عن طريق مجموعة من الخوارزميات يتم استخدامها على نطاق واسع في مهام التعرف على الصور وملامح الوجه وإعادة إنشاء صوت الشخص بدقة، وتصل أوجه التشابه أو التطابقات في الوجه بدقة ٩٥.٧٧ بالمائة[٢١] ونتناول تصنيف المحتوى المزيف من خلال[٢٢]:

- **التزييف السطحيShallow fakes:**

أ- مقاطع فيديو ذات حركة بطيئة: وهي مقاطع فيديو استُخدم فيها برنامج لتعديل الفيديو لإبطاء سرعة الكلام دون تغير طبقة الصوت. وقد يكون القصد من ذلك هو الإشارة إلى وجود خلل في الشخص المستهدف من الفيديو أو التشديد عى كلمات معينة أو نرة الصوت لتزييف وجهات نظر محددة ولرك انطباعاً خاطئاً لدى الجمهور[٢٣].

ب- تغير التواريخ والمواقع: التلاعب بالتواريخ والمواقع لتظهر مقاطع الفيديو عى أنها حديثة وفي أماكن مختلفة، ما يؤدي إلى انتشار أخبار كاذبة تؤثر على المجتمع والأفراد.

- **التزييف العميق :Deepfakes وهو عملية يجري فيها استبدال الوجه Face Swapping:**

باستخدام تقنيات الذكاء الاصطناعي وتعلم الآلة من خال تدريب خوارزميات الذكاء الاصطناعي على الصور المستخرجة من شبكات منفصلة، ثم إعادة بناء الوجه الجديد وإنشاء الفيديو المطلوب كما يمكن تنفيذ العملية نفسها لإنشاء مقاطع صوتية.

---

[٢١] منة الله كمال موسى دياب، سلوك حماية الخصوصية الرقمية البيومترية لدى مستخدمي تطبيقات التزييف الْعميق من طلبة الجامعات المصرية، المجلة العربية لبحوث الإعلام والاتصال، كلية الإعلام بالجامعة الكندية بالقاهرة، العدد ٣٧- أبريل/ يونيو، ص١٨٤.

[٢٢] عمار ياسر البابلي، المخاطر الأمنية للتزييف العميق وآليات المواجهة، مرجع سابق، ص ٧٠.

[٢٣] دليل التزييف العميق، البرنامج الوطنى للذكاء الاصطناعي، يوليو ٢٠٢١، الامارات العربية المتحدة ومتاح علي:
https://ai.gov.ae/wp-content/uploads/2021/07/AI-Deepfake-Guide-AR-2021.pdf

رابعاً- أنواع التزييف العميق:

١- **تقنية الفيديوهات المفبركة "Deepfakes Videos"**: إذ تحتاج الفيديوهات المزيفة لدرجة عالية من الدقة واستخدام متقن للوسائل التكنولوجية، بالإضافة إلى توافر الوقت اللازم والإمدادات المالية وأيضاً للمهارة الفردية، كالفيديو الخاص بالممثل الأمريكي توم كروز[٢٤] الذي انتشر على تطبيق التيك توك، وحظى بأكثر من ١٥,٩ مليون مشاهدة، وتطلب هذا الفيديو استخدام تقنيات الذكاء الاصطناعي على كثير من الفيديوهات الخاصة بالممثل المشهور والتدرب على إنشائه لمدة شهرين: ويمكن لمحتوى التزييف العميق التلاعب بالانتخابات، **وعلى سبيل المثال:** الانتخابات المتقاربة، يمكن أن يظهر مقطع فيديو يظهر شخصا منخرطا في فعل جنسي أو يدلي ببيان مثير للجدل بشكل خاص ومن المتصور أن مثل هذا الفيديو يمكن أن يؤثر على نتيجة الانتخابات[٢٥].

٢- **تقنية نسخ الصوت Voice Cloning**: وهي طريقة يتم من خلالها التلاعب بالحقائق، حيث تسمح العديد من التطبيقات عبر الإنترنت والهواتف المحمولة للمستخدمين القيام بمحاكاة أصوات المشاهير، مثل تطبيقات Celebrity Voice Cloning وVoicer Famous AI Voice Changer، كواقعة تلاعب برئيس تنفيذي لإحدى شركات الغاز والذي صرَّح بأنه تلقى اتصالاً من شخص انتحل صوت مديره يطلب منه تحويل ٢٢٠ ألف يورو لحساب بنكي في المجر، والاستنساخ الصوتي هو طريقة أخرى يتم بها استخدام التزييف العميق وتتيح العديد من التطبيقات عبر الإنترنت والهاتف[٢٦].

- ومثال على ذلك: تم استخدام تقنية Deepfake بعدة طرق لاستهداف الأشخاص في جميع مناحي الحياة، لم يقتصر استخدامها لإنشاء صور

---

(24) SOURCE: Tom [@deeptomcruise], "Sports!" 2021.
NOTE: As of April 12, 2022, this TikTok video had more than 16.1 million views.

(25) Victor, Daniel, "Your Loved Ones, and Eerie Tom Cruise Videos, Reanimate Unease with Deepfakes," New York Times, March 10, 2021.

(26) TODD C. HELMUS, Ibid., Op. cit

(ISSN: 2537- 0758)

ومقاطع فيديو مزيفة للمشاهير والسياسيين فحسب، بل تم استخدام هذه التقنية أيضًا للاحتيال على الأعمال وسرقة أموالهم، على سبيل المثال: في أواخر عام ٢٠١٩، تعرضت شركة ألمانية للطاقة للاحتيال بمبلغ ٢٢٠ ألف دولار أمريكي بعد أن كان التزييف العميق قادرًا على تقليد الصوت لخلق صوت شخصية تنفيذية رفيعة المستوى يطالب الموظف بالدفع الفور[٢٧].

- قال متحدث باسم شركة التأمين التابعة للشركة لصحيفة "واشنطن بوست": "كان البرنامج قادرًا على تقليد الصوت، وليس الصوت فقط: النغمة، وعلامات الترقيم والتوقف الصوتية، واللهجة الألمانية" ولم يتم إعادة إنشاء الصوت بشكل مثالي فحسب، بل تمت مطابقة المكالمة الهاتفية جنبًا إلى جنب مع بريد إلكتروني مزيف عميق يحاكي المدير التنفيذي المستهدف، مما يضيف طبقة أخرى من الشرعية[٢٨].

٣- **تقنية الصور المزيفة Deepfakes Images**: إذ تأتي هذه الصور على شكل لقطة مصورة لوجه شخص تبدو حية للغاية على الرغم من كونها غير حقيقية، مشيراً لواقعة قيام مسؤول في إدارة الرئيس الأمريكي السابق دونالد ترامب بتركيب صورة للباحثة الروسية كاتي جونز، الباحثة في الشأن الروسي والأوراسي بمركز الدراسات الاستراتيجية والدولية، على حساب في اللينكدإن متصل بشبكة حسابات صغيرة للتأثير في الرأي العام[٢٩].

٤- **تقنية النصوص المفتعلة Generative Text**: إذ يتم استخدام نماذج اللغة

---

[٢٧] معين الميتمي، "التزييف العميق".. مستقبل القوانين المنظمة للبرمجيات الذكية، تقرير جريدة العين الإماراتية الإخبارية، بتاريخ ١٣ مارس ٢٠٢١ ومتاح على:
https://al-ain.com/article/deefacke-the-future-of-smart-software-laws

[28] Chawki, M.: Cybercrime in France: an overview. Computer Crime Research Center. December, 2005. Downloaded January 23rd, 2006, from: http://www.crime-research.org/articles/cybercrime-in-france-overview/ (2005) www.scopus.com.

ITU (2018). Global Cybersecarity Index 2018. Geneva. Studies & Research. P. 14.

[29] TODD C. HELMUS, Ibid., Op. cit

الموجودة بأجهزة الكمبيوتر لإنشاء النصوص المختلفة، وهي التي يمكن أن يستغلها الخصوم **لعمل دعاية لغرض المساس بالأمن القومي** حال استخدامها كسلاح من قبل الخصوم أو الجهات الضارة، ويمكن ل text generator تشغيل شبكات روبوت الوسائط الاجتماعية(٣٠)، كما يمكن لمولدات النصوص تحقيق نفس الغايات على وسائل التواصل الاجتماعي- أو يمكنهم إعادة نتائج محرك البحث على الإنترنت التي تحتوي على أخبار مزيفة تطغى على التغطية الحقيقية لقصة معينة يمكن أن ينظر إليها على أنها محرجة أو ضارة للخصم(٣١).

المطلب الثاني

المخاطر الأمنية والاجتماعية للتزييف العميق وأشكال الخداع

يمثل تنظيم التزييف العميق السياسي تحديًا كبيرًا وتسعى التشريعات إلى حظر التزييف العميق للمسؤولين السياسيين أو المرشحين، وظهرت تقنية التزييف العميق، بالطبع، كواحدة من أكبر تهديدات الأمن الرقمي في السنوات القليلة الماضية، ونتناول المخاطر السياسية للتزييف العميق وأشكال الخداع كالتالى:

أولاً- الخداع العميق للذكاء الاصطناعي وحرب الشائعات:

إن التكنولوجيا الحديثة تلعب أدوارا خطيرة في نشر الشائعات والأكاذيب، بهدف تقويض استقرار الدول، وإسقاط الأنظمة، وبث الفوضى في العديد من مناطق العالم، وقد تحول الذكاء الاصطناعي بالفعل في السنوات الأخيرة، ليكون رافدا رئيسيا في صناعة ما يسمى بـ «الكذب العميق»، وهو نوع من الكذب، يملك القدرة على إنتاج

(30) Linvill, Darren, and Patrick Warren, "Understanding the Pro-China Propaganda and Disinformation Tool Set in Xinjiang," Lawfare Blog, December 1, 2021. As of June 6, 2022: https://www.lawfareblog.com/understanding-pro-china-propaganda-and-disinformation-tool-set-xinjiang

(٣١) سالي يوسف، كيف نواجه استخدام الذكاء الاصطناعي في التضليل المعلوماتي، دراسات، مركز المستقبل للأبحاث والدراسات المتقدمة لا يجوز استخدام تقنية "Deep Fake" لتزييف الفيديوهات، إدارة الفتوي بدار الإفتاء المصري، القاهرة، نشر في ٦ يناير ٢٠٢٢، http://www.dar-alifta.gov.eg/home/index

(ISSN: 2537- 0758)

صور ثابتة ومتحركة وناطقة تماثل الحقيقة[٣٢].

وشاهدنا في الآونة الأخيرة العديد من الفيديوهات المفبركة والمزيفة على مواقع التواصل الاجتماعي المختلفة، كان الهدف منها توجيه رسالة محددة تخدم أفكار الجماعات الإرهابية لتعود بنا لنقطة ما قبل الصفر.. واستخدمت تقنيات حديثة في ترويج الشائعات على جمهور الإنترنت.. فلم تكتف بنشر أخبار كاذبة أو صور قديمة فقط.. بل قامت بالتعديل والفبركة على الفيديوهات مستخدمة برامج وأساليب تستخدم في فنون المونتاج والإخراج السينمائي كبرامج "after –adobe premiere effect"، وبجانب فنون السينما تنتشر وتتطور تقنيات «الديب فيك»، لنكون على أبواب حرب تضليل معلوماتية خطيرة تستخدم أحدث التقنيات التكنولوجية التي عرفها هذا العصر[٣٣].

ثانياً- اختراق التزييف العميق للبصمات البارومترية:

تسببت تطبيقات التَّزْيِيف الْعَمِيق للوجه Deepfake في إثارة القلق بين الشركات والقطاعات الحكومية والاقتصادية التي تعتمد على أنظمة الأمان البيومتري، وذلك لأن التَّزْيِيف الْعَمِيق أصبح مقنعًا بشكل متزايد لخداع المستخدمين وأنظمة كشف الهُوِيَّة البيومتريَّة على حد سواء للاعتقاد بأنها أصلية ولذا كان من العجيب أن ترى مقطعًا مرئيًا للرئيس الأسبق للولايات المتحدة الأمريكية أبراهام لنكولن والمتوفى قبل ما يزيد خمسة عشر عقدًا من الزمن، وهو يتحدث هذه الأيام عن أمور نعيشها، وذلك في "مقاطع مَرْئية مفبركة".

ويمكن القول بأنه يمكن من خلال تقنية التزييف العميق أن تُقام حرب بين دولتين أو أكثر، أو أن تؤدي لاستسلام جنود دولة لأعدائهم أثناء الحرب؛ حيث لا تقتصر هذه التقنية على تزييف صورة المقاطع المَرْئية، بل يمكنها توليد الأصوات أيضًا مطابقة للشخص المستهدَف، وفى بداية الغزو الروسي لأوكرانيا في مارس

---

[٣٢] عمار ياسر البابلي، دور الذكاء الاصطناعي في مواجهة الظواهر الإجرامية المُستحدثة عبر طبقات الإنترنت، مجلة الدراسات الأمنية والقانونية، أكاديمية شرطة قطر، عدد الثانى أكتوبر ٢٠٢٤، ص ١٠٢.

[٣٣] تقرير فيسبوك... الذكاء الاصطناعي لمحاربة الأخبار الزائفة ، مجلة (W.D) الدولية ومتاح على: https://p.dw.com/p/34xGP (تاريخ الزيارة ٢٠٢٢/١/٢٩).

٢٠٢٢[٣٤]، ظهر مقطع فيديو مفبرك (Deepfake) للرئيس الأوكراني فولوديمير زيلينسكي على وسائل التواصل الاجتماعي، يأمر مواطنيه بإلقاء أسلحتهم مقاطع مَرْئية مفبرك عبر تقنية التزييف العميق والشعب إلى الاستسلام للقوات الروسية الغازية لبلاده وبعد لحظات، نشر Zelenskyy الحقيقي مقطع فيديو على Facebook لتوضيح الرسالة السابقة على أنها مزيفة تم التلاعب بها، وأشار الخبراء إلى أن هذا المثال بالذات كان غير واقعي نسبيًا ومع ذلك، بمرور الوقت، ستصبح مثل هذه المحاولات أكثر انتشارًا ويصعب اكتشافها مع تحسن التكنولوجيا[٣٥].

ومنذ بداية الحرب في ٢٤ فبراير ٢٠٢٢م تعرضت أوكرانيا لهجمات سيبرانية متنوعة، مثل: هجمات التصيد الاحتيالي، وهجمات رفض الخدمة الموزعة "DDoS"– وقد استهدفت هذه الهجمات بصورة أساسية قطاع الاتصالات وعمليات توزيع الأدوية والمواد الغذائية وإمدادات الإغاثة، وتراوح تأثيرها من منع الوصول إلى الخدمات الأساسية إلى سرقة البيانات ونشر المعلومات المضللة من خلال تكنولوجيا التزييف العميق[٣٦].

وعلى الرغم من أن تقنية التزييف العميق لا تزال في مراحلها الأولى، إلا أنها قد تشكل تحديات هائلة للأمن السيبراني للمؤسسات أثناء نضوجه "وغالبًا ما يتم دعمها بمعلومات شخصية أخرى مسروقة"، تقدم تقنية التزييف العميق وسيلة متطورة للمجرمين لإنشاء هويات مزيف فإن القياسات الحيوية ليست جيدة حيث يمكن سرقة سماتها وإعادة استخدامها بسهولة من قبل المهاجمين والمحتالين في مواقف العمل

(34) Jakub Przetacznik with Simona Tarpov, Russia's war on Ukraine: Timeline of cyber-attacks, European Parliamentary Research Service, June 2022, on https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf.

(35) Kelsey Farish, Deepfakes and their impact on women, Published 9 August 2021, London– walbrook on:
https://www.dacbeachcroft.com/en/gb/articles/2021/august/deepfakes-and-their-impact-on-women/

(36) Destructive malware targeting Ukrainian organizations, Microsoft, January 15, 2022, on https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/.

(ISSN: 2537- 0758)

عن بُعد، **ويمكن تقليل هذا الخطر من خلال طلب التفاعل الشخصي والبشري لتسجيل السمات البيومترية وإثبات الهوية من قبل منظمة موثوقة لديها خبرة في مثل هذه الأشياء.**

ثالثاً- المخاطر الاسرية للتزييف العميق:

من الواضح أن التزييف العميق غير المرغوب لما له من جانب مظلم ومن المثير أن أكثر من ٩٠٪ من ضحايا التزييف العميق هم من النساء، الذين يتعرضون للتحرش الجنسي عبر الإنترنت أو الإساءة من خلال المواد الإباحية المزيفة غير الحسية، وتتراوح الدوافع من "الانتقام الإباحي" إلى الابتزاز ويشكل التزييف العميق الذي يستهدف السياسيين أو الخطاب السياسي أقل من ٥٪ من أولئك الذين يتم تداولهم عبر الإنترنت[٣٧].

وتوفر صفحات الويب المختلفة الآن إمكانية الوصول إلى خدمات التزييف العميق تشمل المواقع الشهيرة Reface، والذي يسمح للمستخدمين بتبديل الوجوه بالوجوه في مقاطع الفيديو وملفات GIF الموجودة؛ My Heritage، الذي يحرك صور الأقارب المتوفين[٣٨]:؛ وZao، وهو تطبيق صيني يستخدم تقنية التزييف العميق للسماح للمستخدمين بفرض وجوههم على وجه واحد من مجموعة مختارة من شخصيات الأفلام الأكثر شهرة وتسمح صفحة الويب Deep Nude للمستخدمين بتحميل الصور، والتي كانت في المقام الأول للنساء، وتقدم مخرجات يبدو فيها موضوع الصورة عاريا[٣٩]، حيث يمكن لتقنية التزييف العميق الإباحية أن تتراكب بشكل مقنع على وجه محدد فوق وجه ممثل إباحي.

---

[٣٧] عمار ياسر البابلي، دور الذكاء الاصطناعي في مواجهة الظواهر الإجرامية المُستحدثة عبر طبقات الإنترنت، مرجع سابق، ص ١٠٥.

[38] Meenu EG, "Try These 10 Amazingly Real Deepfake Apps and Websites," webpage, Analytics Insight, May 19, 2021. As of October 10, 2021: https://www.analyticsinsight.net/try-these-10-amazingly-real-deepfake- apps-and-websites/

[39] Changsha Shenduronghe Network Technology, ZAO, mobile app, Zao App APK, September 1, 2019. As of October 10, 2021: https://zaodownload.com

رابعاً- أشكال التهديدات السياسية التي تطرحها تكنولوجيا الخداع العميق[٤٠]:

- قد تؤدي فبركة تصريحات مسيئة لسياسيين إلى اندلاع أعمال عنف أو تظاهرات أو حتى توتر العلاقات مع دول أخرى، كما يمكن أن تؤدي إلى تهديدات أوسع للأمن القومي، حيث يمكن استخدامها لإحراج أو تقويض أو استغلال عملاء الاستخبارات، المرشحين للمناصب السياسية.
- خلق مشاهد كاذبة لأحداث عنف أو اعتداء، كمشاهد اعتداء الشرطة على المواطنين، وهو ما قد يستفز مشاعر الجماهير، ويجعلها تخرج في تظاهرات حقيقية ضد أجهزة الدولة، يمكن أن يؤدي انتشار التزييف العميق إلى انخفاض الثقة في المؤسسات الإخبارية البارزة من خلال زرع عدم الثقة حتى في الأشكال المشروعة للأخبار والمعلومات[٤١].
- التأثير على الانتخابات والعملية الديمقراطية من خلال فبركة تصريحات سياسية لمرشحي أحد الأحزاب أو قادة الحزب لا تتلاءم مع توجهات الناخبين، مما قد يدفعه لخسارة هذه الانتخابات.
- فبركة مشاهد كاذبة بهدف الإساءة أو الابتزاز، كوضع صورة شخص في وضع مخل بالقواعد المتعارف عليها، أو وضعه في مكان لا يجب التواجد فيه بهدف الابتزاز أو الحصول على المال أو التشهير.
- التأثير على أسهم الشركات والأعمال من خلال خلق صور وتصريحات مفبركة لمديري هذه الشركات تؤدي إلى الإضرار بأسهم الشركة وبموقفها المالي والاقتصادي.
- **تتوقع شركة الأمن السيبراني "فورس بوينت(Forcepoint)" أن يستخدم مجرمو الإنترنت الخداع العميق لتوليد صور ومقاطع فيديو يُمكن توظيفها**

---

(٤٠) إيهاب خليفة، فرص وتهديدات الذكاء الاصطناعي في السنوات العشر القادمة، تقرير المستقبل: مجلة اتجاهات الأحداث، ابوظبي، الامارات العدد ٢٧، ٢٠١٨، ص ١٤.

(41) Vaccari, Cristian, and Andrew Chadwick, "Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News," Social Media + Society, Vol. 6, No. 1, January 2020.

(ISSN: 2537- 0758)

لطلب فدية، وبالتوازي لذلك، فمن المحتمل تزايد عمليات سرقة البيانات من خلال خداع الموظفين للتخلي عن المعلومات، بما في ذلك: بيانات اعتماد الوصول، والسجلات المالية، والمستندات الضريبية، والملفات الشخصية للعملاء، وغير ذلك، **كما يُتوقع تزايد هجمات التصيد الاحتيالي من خلال نشر مقاطع فيديو تحتوي على البرامج الضارة أو تسجيل الرسائل المصممة لجذب المستخدمين إلى النقر على الروابط كجزء من هجمات التصيد الاحتيالى**[٤٢].

خامساً- استخدامات الذكاء الاصطناعي في نشر المعلومات المضللة[٤٣]:

تقنيات الذكاء الاصطناعي جاهزة للاستخدام في حملات المعلومات المضللة وتمثل مقاطع الفيديو المزيفة تهديدا واضحا، لكن استنساخ الصوت وصور التزييف العميق والنص التوليدي يستحق القلق وقدرات (AI) تقوم عليها أدوات لنشر المعلومات المضللة[٤٤]:

- حيث تتضمن مقاطع الفيديو المزيفة العميقة لقطات معدلة صناعيا تقدم تغييرات في وجوه الأشخاص أو أجسادهم ويتم تطوير صور مقاطع الفيديو الاصطناعية هذه من خلال شبكات الخصومة التوليدية (GANs).
- يتكون نظام GAN من مولد يولد صورا من الضوضاء العشوائية ومميزا يحكم على ما إذا كانت صورة الإدخال أصلية أو أنتجها **المولد المكونان متخاصمان وظيفيا**، ويلعبان دورين متعارضين مثل المزور والمخبر حرفيا وبعد فترة التدريب، يمكن للمولد إنتاج صور مزيفة بدقة عالية[٤٥].

---

[٤٢] رغدة البهي، الخداع العميق: تحديات أمنية وإشكاليات حقيقية، المركز المصري للفكر والدراسات الاستراتيجية (ESCC)، وحدة الأمن السيبراني، نشر بتاريخ ٢٧ مارس ٢٠٢١، ومتاح على https://ecss.com.eg/14200/

[٤٣] سالي يوسف، كيف نواجه استخدام الذكاء الاصطناعي في التضليل المعلوماتي، مرجع سابق.

[44] TODD C. HELMUS, Artificial Intelligence, Deepfakes, and Disinformation, Perspective
EXPERT INSIGHTS ON A TIMELY POLICY ISSUE, The RAND Corporation, July 2022 at: https://www.rand.org/pubs/perspectives/PEA1043-1.html

[45] Atlantic Council's Digital Forensic Research Lab, "#Stop the Steal: Timeline of Social Media and Extremist Activities Leading to 1/6 Insurrection," Just Security, February 10, 2021.

- **وجاء تقرير الامن السيبراني** الصادر عن مؤسسة Startup Deep trace الهولندية في عام ٢٠١٩[٤٦] بان اجمالي ما عثرت علية هو ١٤٦٧٨ فيديو مزيف علي شبكة الانترنت في عشرة أشهر فقط منذ ديسمبر ٢٠١٨ وحتي أكتوبر ٢٠١٩ منها ٩٦% كانت لمواد إباحية شوهدت من قبل ١٣٤ ملايين شخصاً الامر الذي يسير الانتباة حول خطورة لإصطناع فيديو إباحي مزيف لأشخاص عاديين لمجرد أنهم قاموا بنشر صورهم بحسن نية علي أحد وسائل التواصل الاجتماعي[٤٧] ومدي تأثير ذلك علي حقهم في الشرف والاعتبار وهو ما حدث بالفعل في عام ٢٠١٨ حيث إكتشفت طالبة في مدرسة ثانوية أسترالية ان شخصا ما أدخل وجهها في مقاطع فيديو وصور إباحية مزيفة بعد أن بحثت عن نفسها من خلال محرك البحث جوجل الامر الذي ولد لديها أضرار نفسية جسيمة[٤٨].

وفي واقعة أخري أدت إلى إنتحار فتاة مصرية في مقتبل عمرها ١٧ عاما في يناير ٢٠٢٢ بعدما إستغل أحد الشخاص صورها المتاحة على مواقع التواصل الاجتماعي ليصنع محتوي إباحي مزيف لها وتركة يتداول بين أفراد مدينتها فما وجدت ملاذا لصون شرفها وسمعتها سوي الموت[٤٩].

والأمر الذي يبدوا خطيراً في سرعة انتشار الشائعات والأخبار الكاذبة وانتشار فيديوهات التزييف العميق على شبكة الإنترنت ومواقع التواصل الاجتماعى عند استخدام شبكات الجيل الخامس والسادس من الاتصالات (5-6G) الفائقة السرعة.

---

[٤٦] محمود سلامة عبدالمنعم الشريف، جريمة الانتقام الإباحي عبر تقنية التزييف العميق" Deepfakes" والمسؤولية الجنائية عنها، مرجع سابق، ص ٣٧٤.

[47] IVAN MEHTA. A new study says 96% of deepfake videos are porn. Oct 7, 2019. Available at: https://thenextweb.com/apps/2019/10/07/a-new-study-says-nearly-96-of-deepfake-videos-are-porn/

[48] https://www.news.com.au/technology/online/security/teens-google-search-reveals-sickening-online-secret-about-herself/news-story/ee9d26010989c4b9a5c6333013ebbef2

[٤٩] قامت وزارة الداخلية المصرية في ٣ يناير ٢٠٢٢ بالقبض على الجناه فورا و تم تقديمهم للعدالة.. راجع الصفحة الرسمية لوزارة الداخلية على الفيس بوك "جهود الوزارة في يناير ٢٠٢٢".

(ISSN: 2537- 0758)

سادساً- أبرز التحديات الأمنية لاستخدام تطبيقات الذكاء الاصطناعي فيما يلي[٥٠]:-

- **استنساخ الأصوات:** أشارت (بلومبرغ) في تقرير مصور لها ضرورة التعرف على مخاطر الذكاء الاصطناعي من بداياته الأولية حالياً للانتباه لها مستقبلاً وتفادي أضرارها وعرض التقرير تطبيق طالب مكسيكي في جامعة كندية تتصدر عالميا في أبحاث الذكاء الاصطناعي وكشف الطالب عن نجاحه في تطوير برنامج صوتي لا يحتاج إلا إلى لحديث شخص لمدة ثماني دقائق لاستخلاص البصمة له، لتركيب عبارات لم ينطقها وتبدو وكأنها عبارات بصوته، مما يقودنا إلى أنها يمكن استخدام تلك البرامج والتي تعمل عن طريق الذكاء الاصطناعي في ارتكاب جرائم أو تسهيل ارتكابها عن طريق انتحال صفة الأشخاص عن طريق المكالمات أو عن طريق الإنترنت عن طريق المجرمين أو الإرهابيين[٥١].

- **احتمالية اختراق نظم الذكاء الاصطناعي:** إذا يمكن للهجمات السيبرانية أن تخترق نظم الذكاء الاصطناعي العسكرية، بحيث يمكن للجهة المهاجمة في بعض الأحيان أن تسيطر على أحد الروبوتات العسكرية، وإعادة توجيهها، ما يلحق الأضرار بالأفراد أو بالمنشآت التي ليست في دائرة الاستهداف أساساً[٥٢].

- **إمكانية خداع نظم الذكاء الاصطناعي:** حيث برز لدى الأجهزة الأمنية في الدول الغربية للاعتماد على نظم الذكاء الاصطناعي في رصد التهديدات التي تواجه الأمن القومي للدولة وتحديده، والتنبؤ كذلك بالتطورات التي يمكن أن تحدث حول العالم، مثل الثورات أو الاضطرابات الاجتماعية لكن، في حال نجح الدول المعادية في تحديد كيفية عمل هذه الأجهزة، فإنه يسهل عليها بالتالي خداعها من خلال نشر أخبار كاذبة، لتضليلها وقيادتها إلى استنتاجات خاطئة[٥٣].

---

[٥٠] عمار ياسر البابلي، تطبيقات الذكاء الاصطناعي في العمل الأمني، مجلة الأمن والقانون، علمية محكمة، أكاديمية شرطة دبي، العدد (١)، يناير ٢٠٢١، ص ٥٤.

[٥١] رغدة البهي، الخداع العميق، المركز المصري للفكر والدراسات الاستراتيجية (ESCC) مرجع سابق.

[52] Triplett, William J. 2022. "Addressing Human Factors in Cybersecurity Leadership" Journal of Cybersecurity and Privacy 2, no. 3: 573-586. https://doi.org/10.3390/jcp2030029 www.scopus.com

[٥٣] إيهاب خليفة، الحرب السيبرانية، الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، مرجع سابق، ص ٢٠١.

المبحث الثانى
آليات مواجهة التزييف العميق

إن الأمر يتطلب مزيجًا من الدفاع التكنولوجي والمسؤولية والوعي البشري لمكافحة هذا الطوفان الجديد من الأخبار المزيفة، التي تهدد نسيج المجتمعات، ويجب أن يتم تعميم وتوعية المواطنين في كل مناسبة بمخاطر وسبل التصدي للتزييف العميق بالطريقة نفسها التي يتم بها التعامل مع مخاطر برامج الفدية أو خرق البيانات فيما سيعد خطوة أولى نحو مكافحة المعلومات المضللة وحماية الأسر والمجتمعات.

ومن الضروري تحديد مصدر أو أصل لقطات التزييف العميق، الامر الذي يرشدنا لإستخدام تقنيات blockchain لتتبع وتحديد أصل الوسائط الرقمية التي تساعد في التعرف الفعال على فيديو التزييف العميق وحساب عامل ثقة المستخدم، ومع انتشار استخدامات تقنيات الذّكاء الاصطناعي في شتى المجالات، وفي أكثر مجالات ال– حياة؛ كان من الواجب بيان التكييف الفقهي لهذه الاستخدامات، والتفريق بين المشروع نظرًا لانتشارها مع (Deepfake) منها وغير المشروع، ومن ذلك تقنية التزييف العميق استخداماتها السيئة المؤدية إلى مفاسد متعددة؛ كالتلاعب بالأدلة الجنائية، وإثارة الفوضى، والإضرار بالأمن القومي للدول، ومن ذلك استخدامها في قذف الغير، وما يتبعه من الابتزاز الجنسي والمالي لضحايا هذه التقنية.

ومع استخدام الذكاء الاصطناعي بدأت تظهر العديد من الحلول العملية من الباحثين الأكاديميين، بالإضافة إلى شركات التكنولوجيا الراسخة مثل Adobe و Microsoft، وشركات التوسع الأحدث مثل https://truepic.com/، حيث تقوم بعض الأدوات بإنشاء بيانات وصفية معينة (مثل "العلامات المائية") عند نقطة الإنشاء، بحيث يمكن التحقق من أنها أصلية في وقت لاحق، بينما تبحث الأدوات الأخرى عن الانحرافات والتحف الرقمية الأخرى لمساعدة المستخدمين على تحديد الصور التي تم التلاعب بها. وفي فبراير ٢٠٢١، تم تأسيس "التحالف من أجل إنشاء المحتوى وأصالته" (C2PA) بواسطة Adobe، جنبًا إلى جنب مع arm و BBC و Intel و Microsoft و truepic.com تسعى إلى صياغة معايير تقنية مفتوحة وخالية من حقوق الملكية لمكافحة المعلومات المضللة.

والحفاظ على الأمن السيبراني هو امر حتمي لتحقيق رحلة تحول رقمي آمنة في الدول، فعلى الرغم من التحديات التي فرضها وباء فيروس كورونا إلا أنها في الوقت

(ISSN: 2537- 0758)

نفسه أظهرت حقائق عديدة وكشفت عن فرص جديدة غيرت من مجريات حياتنا اليومية، فأصبح أمن الفضاء السيبراني الركيزة الأساسية لأيّ تحول رقميّ، حيث تستند إليه المصداقية الرقمية للشركات والمؤسسات[٥٤].

كما يقصد بالأمن السيبرانى: التكنولوجيا والعمليات والضوابط الهادفة إلى حماية الأنظمة والشبكات والبرامج من الهجمات الرقمية ومنها التزييف العميق والخداع، فيُلعب الأمن السيبرانى دوراً جوهرياً "محورياً" فى مواجهة التحديات ويدعم الأمن السيبرانى النمو الاقتصادي من خلال الحفاظ على أهمية الرقمنة وزيادة الثقة بها[٥٥]، **ونتناول هذا المبحث كالتالي:**

المطلب الأول
المواجهة القانونية لجرائم التزييف العميق

يتعلق الأمن السيبرانى فى جانب كبير منه بالأمن القومي لأي دولة، فكل دولة تحتفظ بالضرورة بحقها وسيادتها الكاملة على فضائها السيبرانى، وهو ما يبرز ضرورة تدخل الدول لحماية سيادتها على فضائها الإلكترونى وأمنها السيبرانى، عن طريق المواءمة والتنسيق بين الدول الأخرى، واحترام سيادة كل دولة، وفى إطار من الشرعية القانونية على المستوى الدولى والوطنى على حدٍ سواء ونتناول المواجهة الدولية والقانونية لجرائم التزييف العميق كالتالى:

الأول- موقف المشرع المصري من التزييف العميق:

جرم المشرع المصرى فعل التزييف العميق فى قانون جرائم تقنية المعلومات حيث جاء فى الفصل الثالث منه بعنوان الجرائم المتعلقة بالإعتداء على حرمة الحياة الخاصة والمحتوى المعلوماتى غير المشروع حيث نص فى الفقرة الأخيرة من **المادة (٢٥) من القانون رقم ١٧٥ لسنة** ٢٠١٨ بشأن مكافحة جرائم تقنية المعلومات[٥٦] إليه على أن: "يعاقب بالحبس مدة لا تقل عن ستة أشهر، وبغرامة لا تقل عن

---

[٥٤] كلاوس شواب، الثورة الصناعية الرابعة، ملخصات مؤسسة محمد بن زايد للمعرفة، دبي، الإمارات، ٢٠٢٠، ص٢.

[55] Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers and Security, 38, 97 www.scopus.com

[٥٦] قانون رقم ١٧٥ لسنة ٢٠١٨ بشأن بمكافحة جرائم تقنية المعلومات، الجريدة الرسمية، القاهرة، نشر بتاريخ ١٤– ٠٨– ٢٠١٨.

خمسين ألف جنيه ولا تجاوز مائة ألف جنيه، أو بإحدى هاتين العقوبتين كل من إعتدى على المبادئ أو القيم الأسرية فى المجتمع المصرى أو إنتهك حرمة الحياة الخاصة، أو أرسل بكثافة العديد من الرسائل الإلكترونية لشخص معين دون موافقته، أو منح بيانات شخصية إلى نظام أو موقع إلكترونى لتوريد السلع أو الخدمات دون موافقته، أو نشر عن طريق الشبكة المعلوماتية أو بإحدى وسائل تقنية المعلومات معلومات أو أخبارًا أو صورًا وما فى حكمها، تنتهك خصوصية أى شخص دون رضاه، سواء كانت المعلومات المنشورة صحيحة أو غير صحيحة".

كذلك كانت المادة ٢٦ من ذات القانون أكثر دقة فى توصيف بعض صور التزييف العميق حيث نصت على أنه: "كل من تعمد إستعمال برنامج معلوماتى أو تقنية معلوماتية فى معالجة معطيات شخصية للغير لربطها بمحتوى مناف للآداب العامة، أو لإظهارها بطريقة من شأنها المساس بإعتباره أوشرفه".

يتفق ذلك مع نص قانون حماية خصوصيَّة البيانات الشخصيَّة الرَّقميَّة رقم ١٥١ لسنة ٢٠٢٠؛ حيث يعرف البيانات الشخصيَّة بأنها: أية بيانات متعلقة بشخص طبيعيّ محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخرى: بالاسم، أو بالصوت، أو بالصورة، أو برقم تعريفي، أو محدد للهوية عبر الإنترنت، أو أي بيانات تحدد الهُوِيَّة النفسيَّة، أو الصحية، أو الاقتصاديَّة، أو الثقافيَّة، أو الاجتماعيَّة، ويعد تصميم تطبيقات بيومتريَّة أكثر تعقيدًا– تعتمد على عمليات مسح البصمات الرَّقميَّة، وفحوصات التعرف على الصور، بالإضافة إلى تحسين أداء الصور والكلام– أمر في غاية الخطورة، وانتهاك خصوصيَّة المستخدم دون اعتبار لحقوق المستخدمين في الخصوصيَّة، والحق في حماية البيانات، والتي تعد من حقوق الإنسان الأساسية في ظل تنامي مشكلة انتشار المعلومات المضللة عبر الإنترنت[٥٧].

ثانياً- موقف المشرع الإماراتى من جرائم التزييف العميق:

دخل قانون الجرائم الإلكترونية الجديد، الذي تم تبنيه بموجب المرسوم بقانون اتحادي رقم ٣٤ لعام ٢٠٢١، حيز التنفيذ في ٢ يناير ٢٠٢٢ ليحل محل القانون

[٥٧] منة الله كمال موسى دياب، سلوك حماية الخصوصية الرقمية البيومترية لدى مستخدمي تطبيقات التزييف الْعميق من طلبة الجامعات المصرية، مرجع سابق.

(ISSN: 2537- 0758)

الاتحادي السابق رقم ٥ لعام ٢٠١٢ بشأن مكافحة جرائم تقنية المعلومات، وذلك للحفاظ على الأمن القومي الاماراتى، وغلّظ قانون مكافحة جرائم تقنية المعلومات الجديد، الصادر وفق مرسوم بقانون اتحادي رقم ٣٤ لسنة ٢٠٢١ في شأن مكافحة الشائعات والجرائم الإلكترونية، العقوبات بشأن جرائم بعينها، من بينها الإضرار بأنظمة المعلومات بالجهات المصرفية أو الإعلامية أو الصحية والعلمية وكذلك مؤسسات الدولة والمرافق الحيوية، لتصل إلى السجن المؤقت وغرامة لا تقل عن ٥٠٠ ألف درهم ولا تزيد على ثلاثة ملايين درهم[٥٨].

ويوضح القانون الجرائم والعقوبات ضد أي شخص قد ينشئ أو يستخدم موقعًا إلكترونيًا أو أي وسيلة تقنية معلومات لاختراق نظم المعلومات والبيانات الحكومية أو مهاجمتها أو العبث بها، أو نشر معلومات كاذبة، أو معلومات تضر بمصالح وأمن دولة الإمارات. يتناول القانون جرائم إلكترونية أخرى تشمل **أهمها:**

- إنشاء أو تعديل روبوتات إلكترونية لنقل بيانات زائفة في الدولة أو تزوير المستندات الإلكترونية- الاعتداء على البيانات والمعلومات الشخصية والتلاعب بالبيانات الطبية والحسابات المصرفية والأكواد السرية- التسول الإلكتروني.
- نشر بيانات أو معلومات لا تتوافق مع معايير المحتوى الإعلامي وإتاحة محتوى غير قانوني والامتناع عن إزالته، وإنشاء أو إدارة موقع إلكتروني للاتجار بالبشر، التحريض على الفجور، ونشر مواد إباحية والمساس بالآداب العامة- تحويل، أو حيازة، أو استخدام أو اكتساب أموال غير مشروعة.
- الاحتيال الإلكتروني- الابتزاز والتهديد الإلكتروني- السب والقذف وإجراء المسوحات الإحصائية أو الدراسات الاستطلاعية دون ترخيص والإعلان أو الترويج المضلل للمستهلك- الترويج لمنتجات طبية دون ترخيص والدعوة والترويج لمظاهرات دون ترخيص- التحريض على عدم الانقياد للتشريعات.

---

[٥٨] مرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ في شأن مكافحة الشائعات والجرائم الإلكترونية ومتاح علي:

https://laws.uaecabinet.ae/ar/materials/law/1526

وضعت دولة الإمارات العربية المتحدة قانون ترويج الشائعات ليكون رادعاً يتصدّى لكل من يرغب بنشر البلبلة وقلب الحقائق لأهداف شخصية، من أجل افتعال الخراب بين المواطنين، بحيث يتضمّن هذا القانون بين كفّتيه عقوبة نشر الشائعات التي سيتم تطبيقها على كل من له يد في نشرها دون استثناء.

وبناءً على قانون ترويج الاشاعات المادة ١٩٧ مكرر ٢، فإن كل من استعمل أي وسيلة من وسائل الاتصال وتقنية المعلومات في نشر معلومات وأخبار تعرّض أمن الدولة للخطر وتهدّد أو تمس النظام العام فيها، سيعاقب بالسجن المؤقت على جريمته.

وجاءت المادة ١٩٨ مكرر بأنه[٥٩] تتمثّل عقوبة ترويج الشائعات في دولة الإمارات بحبس مروّج الإشاعة لمدة لا تقلّ عن سنة في حال أذاع أخباراً كاذبة، بهدف زعزعة الأمن العام أو زرع القلق والرعب في الناس أو إلحاق أي ضرر بالمصلحة العامة، ويعاقب بذات العقوبة كل من حاز بالذات أو بالوساطة أو أحرز محرّرات أو تسجيلات أو مطبوعات تتضمّن أخباراً ومعلومات كاذبة، يجدر بالذكر أن عقوبة مروجى الاشاعات تتمثّل بالسجن المؤقت في حال كان الجاني من القوات.

ثالثا- موقف المشروع الأوروبي:

- وضع الاتحاد الأوروبى فى اغسطس ٢٠١٦م نظاماً يسمى (توجيه الاتحاد الأوروبى حول أمن الشبكات والمعلومات) NIS، ويُعد أول تشريع على مستوى الاتحاد الأوروبى حول حماية الأمن السيبرانى، واشتمل على مجموعة من الضوابط الأمنية المتعلقة بحماية الأمن السيبرانى، إذ يطلب من شركات قطاعات البنية التحتية، ومشغلى الخدمات الأساسية، ومقدمى خدمات البيانات، ضمان مستوى من الأمن يتناسب مع الخطر الذي يمثله تقديم الخدمات المشمولة، مع مراعاة أمن النظم والمرافق، والتعامل مع الحوادث.
- تتطلب معالجة الجوانب الموضوعية للحماية الجنائية للأمن السيبرانى تحديد البناء القانونى لهذه الجرائم، ومنهج وصور التجريم، وضوابط وقواعد المسؤولية

[٥٩] مرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ في شأن مكافحة الشائعات والجرائم الإلكترونية.

(ISSN: 2537- 0758)

الجنائية، وفق منهج وخطة الأنظمة القانونية الحديثة وتعاقب بمقتضاها على صور السلوك غير المشروع الذي يمثل خللاً بمصالح الأمن السيبرانى ومنها:

١- **قانون الخدمات الرقمية الأول:** جاءت اللائحة الجديدة الصادرة عن الاتحاد الأوروبي تقوم على التزام الشركات التكنولوجية الكبرى **التعامل الفوري مع المعلومات المضللة** التي تحفل بها منصاتها، وهي اللائحة المدعومة من قبل "قانون الخدمات الرقمية"، وجاء قانون الخدمات الرقمية الأول من نوعه في العالم وهدفه التنظيم الرقمي للشركات العملاقة المالكة لمنصات التواصل الاجتماعي، وبنود القانون تحمي الفضاء الرقمي من أخطار المحتوى غير القانوني حماية للحقوق الأساسية للمستخدمين في أوروبا وسيتعين على هذه المنصات إزالة أي محتوى مسيء أو غير قانوني يتعارض وقوانين الدول الأوروبية **مثل التنمر والكراهية والتضليل والتحرش** و"يجبر" القانون الجديد المنصات الرقمية على مراعاة قدر أكبر من الشفافية في خوارزميات المقترحات أو التوصية التي تعرضها أمام المستخدمين لغرض توجيههم لمنتج أو محتوى بعينه، وألا تُبنى المقترحات على أساس دين أو جنس أو هوية المستخدم(٦٠).

رابعاً- موقف المشرع الأمريكي:

تم اعتماد العديد من مشاريع القوانين على مستوى الولايات في الولايات المتحدة. في عام ٢٠١٩، أصدرت تكساس قانونا من شأنه أن يجعل من غير القانوني توزيع مقاطع فيديو التزييف العميق التي تهدف إلى "إصابة مرشح أو التأثير على نتيجة الانتخابات" في غضون ٣٠ يوما من الانتخابات (الهيئة التشريعية لولاية تكساس SB-٧٥١، ٢٠١٩)(٦١).

---

(٦٠) أمينة خيري، التزييف عميق والتضليل شديد في عصر التمكين الرقمي، موسوعة "Independent Arabia"، بتاريخ ١٥ يوليو ٢٠٢٢ ومتاح على:

https://www.independentarabia.com/node/351936/

(61) Cheng, Eric C. K., and Tianchong Wang. 2022. "Institutional Strategies for Cybersecurity in Higher Education Institutions" *Information* 13, no. 4: 192. https://doi.org/10.3390/info13040192 www.scopus.com

وقد قامت ولاية فرجينيا بفرض عقوبات جنائية على فديوهات التزييف العميق وخاصة الإباحية المزيفة بدون موافقة ذوى الشأنة وبقصد الإكراه أو المضايقة، ذلك القانون الذى دخل التنفيذ فى ١ يوليو ٢٠١٩، وقام القانون بتجريم اصطناع أو بيع أو توزيع مقاطع الفيديو الإباحية المفبركة جنحة من الدرجة الأولى، يعاقب عليها بالسجن لمدة تصل إلى عام وغرامة قدرها ٢٥٠٠ دولار، وفى الأول من سبتمبر ٢٠١٩، وجرمت **ولاية تكساس:** إنشاء أو توزيع مقاطع فيديو مزيفة من خلال إدخال تعديل على قانون الانتخابات لديها بإضافة نص جديد يجرم هذا الفعل إذا قصد منه إيذاء مرشح معين أو التأثير على نتيجة الانتخابات حال نشرها وتوزيعها خلال ٣٠ يوماً من الانتخابات واعتبرت هذا الفعل كذلك جنحة من الدرجة الأولى يعاقب مرتكبها بالسجن لمدة عام فى أحد سجون الولاية وغرامة تصل إلى ٤٠٠٠ دولار[٦٢].

المطلب الثانى

الآليات التقنية والأمنية لمواجهة التزييف العميق

تتوفر تقنيات عدة لمساعدة المستخدمين الذين لديهم خبرات في التحقق على التمييز بين المحتوى الحقيقي والمزيف، فمعظم الأنظمة المستخدمة والقائمة على **التعلم العميق لكشف التزييف العميق** تعتمد البحث في البيانات الخام للعثور على علامات عدم الأصالة وتحديد الخطأ في الفيديو غير أن البرامج المستخدمة لتوليد التزييف العميق تتطور بشكل مستمر وأصبح من الصعب كشف التزييف، ونتناول أحدث الأليات لمواجهة التزييف العميق كالتالى[٦٣]:

أولاً- قدرة الذكاء الاصطناعى على اكتشاف التزييف العميق:

يستفيد الذكاء الاصطناعي من مجموعة متنوعة من التقنيات، مثل تعلم الآلة وتعلم العمق والشبكات العصبية الاصطناعية، لاكتشاف أنماط غير طبيعية أو

---

[٦٢] محمود سلامة عبد المنعم الشريف، جريمة الانتقام الإباحي عبر تقنية التزييف العميق" Deepfakes" والمسؤولية الجنائية عنها، مرجع سابق، ص ٣٧٤.

[٦٣] عمار ياسر البابلي، الذكاء الاصطناعي في مواجهة الشائعات وجرائم تمويل الإرهاب في البيئة السيبرانية "التداعيات وسبل المواجهة"، المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، القاهرة، ٢٠٢٣، ص١٢٤.

(ISSN: 2537- 0758)

تلاعب في المحتوى وهناك عدة طرق يستخدمها الذكاء الاصطناعي لاكتشاف التزييف العميق:

١- **تحليل البيانات واستخراج المعلومات:** يمكن (AI) مساعدة المحققين في تحليل البيانات المرتبطة بالمحتوى المشكوك فيه لاكتشاف أي علامات تدل على التزييف العميق، مثل التلاعب بالصور أو الفيديوهات.

٢- **تعلم الآلة وتعلم العمق:** يمكن تدريب (AI) على مجموعة كبيرة من البيانات الأصلية والموثوقة ليتعرف على الأنماط الطبيعية والمعتادة. ومن ثم يستخدم هذه الأنماط لاكتشاف الاختلافات والتلاعبات في المحتوى الذي يُشتبه في أنه مزيف.

٣- **الكشف عن العلامات الرقمية:** يمكن أن يُضاف توقيع رقمي إلى المحتوى الأصلي للكشف عن أي تغييرات أو تعديلات. يمكن (AI) مقارنة العلامات الرقمية للمحتوى المشبوه بتلك الموجودة في المحتوى الأصلي لتحديد مدى صحته.

٤- **الكشف عن النص الزائف:** يمكن (AI) مساعدة في الكشف عن النصوص الزائفة أو المضللة، سواء في المقالات أو الرسائل أو المشاركات على وسائل التواصل الاجتماعي

٥- **توليد البيانات في تقنية :Deepfake** هذه التقنية تستخدم خوارزميات الذكاء الاصطناعي من شبكات تعرف بالـ Generative Adversarial Networks، وشبكات الخصومة التوليدية وهي مجموعة من الخوارزميات التي تقوم بالتعلّم الاستنتاجي، هذا التعلم يتيح لخوارزميات تعلم الآلة التعلّم عن طريق تمييز أنماط البيانات دون أن تكون هذه البيانات مسمات أو المعرفة[٦٤].

نظام توليد البيانات في تقنية Deepfake هو عبارة عن نموذج يستخدم خوارزميات الذكاء الاصطناعي لإنشاء محتوى مزيف يبدو وكأنه أصلي. يُعتبر Deepfake تطبيقاً شائعاً لتقنية شبكات التآمر الإنشائية (Generative

[٦٤] نايلة الصليبي، إنتل تطور أداة جديدة لكشف التزييف العميق ومحاربة التضليل، مجلة علمية مونت كارلو الدولية (MCD)، نشر في ٢٠٢٢/١١/٢٤:
https://www.mc-doualiya.com/

Adversarial Networks أو GANs)، وهو يُمثل تحسيناً متقدماً في مجال توليد الصور والفيديوهات المزيفة.

في Deepfake، يتم استخدام مولِّد (Generator) لإنشاء الصور والفيديوهات المزيفة، ويتم استخدام مميز (Discriminator) لاكتشاف الفروق بين المحتوى الأصلي والمزيف. يتم تدريب هذين العنصرين بشكل متزامن، حيث يحاول المولِّد توليد محتوى يبدو وكأنه أصلي بحيث يمكن خداع المميز، فيما يحاول المميز تمييز الصور الأصلية من الصور المزيفة. تستمر هذه العملية حتى يتم الحصول على نتائج تجعل المحتوى المزيف غير قابل للكشف أو التمييز بسهولة.

يجب ملاحظة أن تقنية Deepfake يمكن استخدامها بأشكال إبداعية ومفيدة، مثل في مجال الفنون أو الترفيه، ولكنها أيضًا قد تستخدم بطرق غير أخلاقية أو ضارة، مثل نشر محتوى مزيف لتشويه صورة شخص ما أو انتشار أخبار كاذبة. لذلك، تحظى هذه التقنية بالاهتمام والدراسة للتعرف على طرق اكتشاف العمليات المزيفة ومواجهة تحدياتها[٦٥].

ثانياً- مكافحة الخداع العميق Deepfake:

تكمن الفكرة الأساسية في تدريب مجموعة من **الشبكات العصبية الاصطناعية**، المكون الرئيسي لخوارزميات التعلم العميق، على أمثلة متعددة للممثل والوجوه المستهدفة، ومن خلال التدريب الكافي، ستتمكن **الشبكات العصبية** من إنشاء تمثيلات رقمية لميزات كل وجه، ثم إعادة توصيل الشبكات العصبية لتعيين وجه الممثل على الهدف[٦٦].

١- يبحث **Facebook** في اكتشاف التزييف العميق لمنع انتشار الأخبار المزيفة على شبكته الاجتماعية، وأطلقت وكالة مشاريع الأبحاث الدفاعية المتقدمة (DARPA)، الذراع البحثية لوزارة الدفاع الأمريكية، أيضًا مبادرة لوقف التزييف العميق وأدوات التضليل الآلي الأخرى، وقد أطلقت Microsoft أداة الكشف عن

---

[٦٥] شادي عبد السلام، حروب الجيل الخامس: أساليب التفجير من الداخل على الساحة الدولية، مرجع سابق، ص١٢٢.

[٦٦] إيهاب خليفة، الحرب السيبرانية، الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، دار العربي للنشر والتوزيع، القاهرة، ٢٠٢١، ص ٢٠٦.

(ISSN: 2537- 0758)

التزييف العميق قبل الانتخابات الرئاسية الأمريكية[٦٧].

٢- نفترض أنه عندما يتحدث الشخص، يكون لديهم تعبيرات وحركات وجه مميزة (ولكن ربما ليست فريدة)، بالنظر إلى مقطع فيديو واحد كمدخل، نبدأ بتتبع حركات الوجه والرأس ثم استخراج قوة وحدات عمل معينة- ثم نبني نموذجاً للكشف الذي يميز الحقيقة، مثل خوارزميات التعرف على الوجه وحركا الوجه المميزة داخل مقطع الفيديو الواحد.. حيث يتم تسجيل كافة حركات الوجه والرأس ويتم تتبع قياس حجم الوجه والأنف والجبين في (الثلاثي الأبعاد) والأوضاع المختلفة، حركات عضلات الوجه- الفك- الأسنان- الشفاه وميض العين-زوايا حركات الكلام والحواجب، وتكبير حركات الفم والشفاه **ومضاهاتها بالنسخة الأصلية** لاكتشاف تزامن تحريك الشفاه، وهل يبدو الأمر منطقيا، ثم تعزيز المهارات السمعية والمرئية، يتضح من كل ما ذُكر أن الأمر يتعلق بحواس الإنسان وخاصة المهارات السمعية والمرئية.

٣- يتم عمليات التحليل والنمذجة مع التسجيل الزمنى للتوافق العضلي العصبي أثناء حركات الكلام، وكذا دورات الرأس.. ويقوم نماذج التعليم العميق **بمضاهاة الفيديوهات بفيديوهات سابقة للأشخاص أو الأماكن التي ظهرت في الفيديوهات** المراد التحقق من صحتها باستخدام الشبكات العصبية التي تتحدث مع بعضها البعض للبحث عن الأشخاص داخل الفيديوهات على فيديوهات مماثلة على شبكة الإنترنت والـ **you tube**، وبالتالي: يتم إنشاء مجموعات كبيرة من البيانات والفيديوهات والمقاطع الأصلية- ونجد أن أنظمة الذكاء الاصطناعي والمستقبلية في التعليم العميق (deep learning) من عمليات البحث والمضاهاة والتأكد من مصدقيه الفيديو.

٤- **تقنية تسمى "الهندسة العكسية"** تقوم على تفكيك طريقة صنع منتج ما، وفي هذه الحالة مقطع فيديو أو صورة، وترصد البرمجية التي يستعين بها النظام أي ثغرات على عملية التوليف (المونتاج) تؤثر على البصمة الرقمية للصور، وفي مجال التصوير الفوتوغرافي، تتيح هذه البصمة التعرف إلى الكاميرا المستخدمة،

---

[٦٧] رغدة البهي، الخداع العميق، المركز المصري للفكر والدراسات الاستراتيجية (ESCC) مرجع سابق.

وفي المعلوماتية، يمكن لهذه التقنية "التعرف إلى النظام المستخدم في صنع عمليات التزييف، وقدمت شركة "مايكروسوفت" في ٢٠٢٢ برمجية من شأنها المساعدة في رصد عمليات **التزييف العميق**" في الصور أو الفيديوهات، وهي من البرامج الكثيرة المصممة للتصدي للتضليل الإعلامي قبل الانتخابات الرئاسية الأميركية(٦٨).

٥- وبتطوير أدوات ذكاء صناعي للتعامل مع العناصر، التي تحدد السمات والسلوكيات، بما يشمل الطرق الدقيقة لإمالة الرؤوس أو تحريك الشفتين والفم، لإنتاج ما أطلقوا عليه تسمية ملف شخصي ذو "بصمات ناعمة "، نسبة دقة ٩٢% **(لمحاولة اكتشاف الفيديوهات المزيفة).**

ثالثاً- أبرز التقنيات الذكاء الاصطناعي لكشف تهديدات التزييف العميق:

١- طور مختبر **إنتل**، تقنية Fake Catcher قادرة على اكتشاف مقاطع الفيديو المزيفة بمعدل دِقَّة يبلغ ٩٦% بالمئة، ودائما حسب شركة إنتل "هو أول نظام يمكنه كشف التزييف العميق آنيا وتصنيف مقاطع الفيديو والصوت المزيفة بوقت قياسي يبلغ الأجزاء من الثانية"، ويشير مختبر إنتل للذكاء الاصطناعي أن الذي يميز تقنية Fake Catcher عن غيرها المستخدمة، هو اعتماد البحث عن أدلة حقيقية في مقاطع الفيديو الحقيقية إذ يستخدم العين والنظرة ورفة العين، وأيضا إشارات تدفق الدم، التي تجمع من الوجه بالكامل وبعد ذلك بعد تترجم الخوارزميات هذه الإشارات إلى خرائط مكانية-زمانية يكتشف Fake Catcher بمساعدة التعلّم العميق، على الفور ما إذا كان الفيديو حقيقيًا أم مزيفًا(٦٩).

٢- **نظام الكشف GAN٢٠٢١ وطلب** نظام GAN على كل من المُولد، الذي ينشئ الصور والتمييز، الذي يحدد الصور التي تم إنشاؤها أصلية أو مزيفة وتسعى برامج تطوير قدرات الكشف إلى بناء أدوات تمييز فعالة بشكل متزايد

---

(68) https://stringfixer.com/ar/Reverse-engineer

(٦٩) إنتل هي عضو في تحالف من أجل إنشاء المحتوى وأصالته The Coalition for Content Provenance and Authenticity (C2PA)، الذي يركز على معالجة المعلومات المضللة على الإنترنت من خلال تطوير المعايير التقنية للمصادقة على مصدر وتاريخ المحتوى المنشور. يضم التحالف هذا شركات Truepic Microsoft, Intel, Arm, Adobe.

(ISSN: 2537- 0758)

للكشف عن محتوى التزييف العميق، وقامت وكالة مشاريع البحوث وزارة الدفاع الأمريكية باستثمارات كبيرة في تقنيات التطوير من خلال برنامجين متداخلين: برنامج الطب الشرعي الإعلامي، الذي اختتم في عام ٢٠٢١، وبرنامج الطب الشرعي الدلالي تلقى برنامج Sema– For تمويلا بقيمة ١٩.٧ مليون دولار للسنة المالية ٢٠٢١ وطلب ٢٣.٤ مليون دولار للسنة المالية ٢٠٢٢[٧٠] وعقد Facebook "مسابقة تحدي التزييف العميق"، حيث قام أكثر من ٢,٠٠٠ مشارك بتطوير واختبار نماذج لتفكيك التزييف العميق[٧١]، وتعمل شبكات GAN على تحسين دقة الصورة التي يمكنها إنشاؤها ستصبح التزييف العميق والصور الحقيقية غير قابلة للتمييز وحققت أجهزة الكشف دقة بنسبة ٨٢ في المائة عند اختبارها مقابل مجموعة بيانات عامة من التزييف العميق.

٣- **محرك GOOGLE**: يمكن للمستخدم المساعدة في التحقق من صحة صورة أو مقطع فيديو مريب عن طريق التقاط لقطة شاشة للصورة أو الفيديو وتشغيله من خلال Google أو منصة البحث العكسي عن الصور التابعة لجهة خارجية، حيث يقدم محرك جوجل **التحليل الجنائي** للصور في المحتوى امتدادا للويب يسمح للمستخدمين بتجميد مقاطع الفيديو ذات الإطار، وإجراء عمليات بحث عكسية عن الصور على إطارات الفيديو، تكبير صور الفيديو المجمدة مساعد التحقق من الصور لمحاولته لبناء "أداة شاملة للتحقق من الوسائط" ويقدم العديد من الأدوات، بما في ذلك اكتشاف العبث بالصور algorithms والبحث العكسي عن الصور وتحليل البيانات الوصفية[٧٢]، ويمكن أن يكشف البحث عن جوانب من المحتوى المشبوه الذي يمكن أن يكون مزيفا.

٤- **BLOCKCHAIN**: تقنية سلسلة الكتل أو بلوك تشين Blockchain أصبحت اليوم حديث الساعة وأصبح لها القدرة على النمو لتصبح حجر الأساس

(70) Salyer, Kelley M., and Laurie A. Harris, "Deep Fakes and National Security," Congressional Research Service, updated June 8, 2021.

(71) A. Ferrer, Cristian Canton, Ben Pflaum, Jacqueline Pan, Brian Dolhansky, Joanna Bitton, and Jikuo Lu, "Deepfake Detection Challenge Results: An Open Initiative to Advance AI," Meta AI, blog, June 12, 2020. As of October 10, 2021:

(72) Invidia and We Verify, Invidia, web browser plugin, Version 0.75.4, February 24, 2022. As of March 24, 2022:
https://www.invid-project.eu/tools-and-services/invid-verification- plugin/

لأنظمة حفظ السجلات والبيانات في جميع أنحاء العالم، سلسلة من السجلات المترابطة مع بعضها البعض، تعرف باسم Blockchain. بمجرد تخزين البيانات لا يمكن تعديله، ويتم تخزين تجزئة الفيديو الأصلي على blockchain، لتوفير مستويات معينة من المصادقة والقبول والتحقق من الصحة، ويجب استخدام التقنيات اللامركزية في تقنيات blockchain، كدفتر أستاذ موزع لامركزي، فإن blockchain لديه القدرة على توفير معلومات ومعاملات آمنة ودقيقة وتتمتع Blockchain بالقدرة على تضمين الوظائف الأساسية التي يمكن استخدامها لإثبات أصالة وأصالة الكائنات الرقمية بطريقة لامركزية وموثوقة للغاية ومستقرة(٧٣)، بلوك تشين blockchain أو سلسلة الكتل هي عبارة عن ما يشبه قاعدة بيانات مشفرة وموزعة وآمنة، تسمح للمشاركين في الشبكة بإنشاء سجل موثوق لبيانات المعاملات دون الحاجة إلى طرف ثالث(٧٤).

٥- وللتخفيف من مخاطر التزييف العميق المعقدة، يجب اتباع نهج متعدد الجوانب. يشمل ذلك الاستثمار في تقنيات اكتشاف التزييف العميق الأكثر تعقيدًا، بالإضافة إلى تحسين أنظمة التحقق من الهوية. يمكن استخدام تقنيات متطورة للتحقق من الهوية، مثل تقنيات المقاييس الحيوية، لمنع استخدام التزييف العميق في سرقة الهوية وتعزيز محو الأمية الإعلامية والتفكير النقدي، وذلك من خلال تثقيف الجمهور حول مخاطر التزييف العميق وكيفية اكتشافها. ويمكن توعية الناس حول الخطر المحتمل لتلك الهجمات وتزويدهم بالمعرفة والمهارات الضرورية للاستدلال والتحقق من صحة المعلومات المشتركة عبر المنصات الإلكترونية.

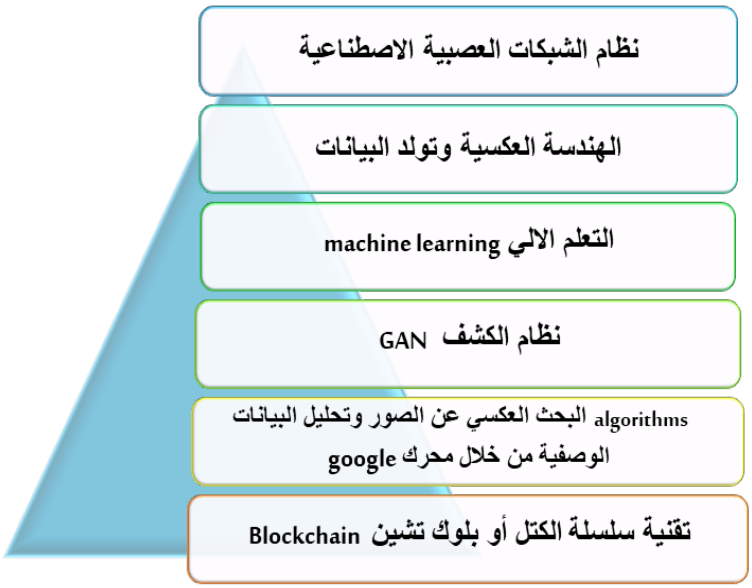
---

(73) MTech, Blockchain Based Approach for tackling Deepfake videos, International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN: 2456-3307 (www.ijsrcseit.com) Doi: https://doi.org/10.32628/CSEIT217372

(74) A. Dhiran, D. Kumar, Abhishek and A. Arora, "Video Fraud Detection using Blockchain," 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), 2020, pp. 102-107.

(ISSN: 2537- 0758)

ويوضح الشكل التالي، قدرة الذكاء الاصطناعى على اكتشاف التزييف العميق



رابعاً- المواجهة الأمنية للدول لترويج الشائعات والتزييف العميق عبر الإنترنت:

التجربة المصرية

١- لقد سعت وزارة الداخلية المصرية انطلاقاً من مسئوليتها الوطنية في خدمة قضايا العمل الأمني إلى تطوير وتحديث فعاليات أداء مختلف الأجهزة الأمنية، فرسالة الأمن الحقيقية تتطلب أداء فعالا، يأخذ بأسباب العلم وتقنياته، وكانت لوزارة الداخلية المصرية التجربة الرائدة حين أنشات مركزا متخصصا للإعلام الأمن بقطاع الإعلام والعلاقات وتجهيزه بأحدث وسائل التقنية، وتزويده بالضباط المتخصصين في مجالات الإعلام، تحقيقا لأهداف فرسالتها الأمنية، وترسيخا لاستراتيجيتها الوطنية، والتخطيط برؤية مستقبلية لقضايا الأمن والتنمية، **تماشيا مع طبيعة المرحلة والمتغيرات والتحديات التي تواجهها وقام بكل من**[٧٥]:

[٧٥] سامر جمال، المردود الأمني للشائعات ودور الشرطة في مواجهتها، دراسة تطبيقية على الإنترنت، رسالة دكتوراه، أكاديمية الشرطة، كلية الدراسات العليا، القاهرة، ٢٠٢١، ص٢٧١.

١- التوسع في استخدام مواقع التواصل الاجتماعي، ولد كان مركز الإعلام الأمني المصري سباقا في هذا المجال، مقارنة بكثير من المؤسسات التي يتم فيها استخدام هذه المواقع باجتهادات لأشخاص أو مسئولين فيها، وليس مهني ومدروس.

٢- انتهاج الأسلوب الأكثر ملاءمة للتعامل مع طبيعية ونوعية الشائعة، فمن غير المعقول أن يكون هناك أسلوب واحد تنتهجه المؤسسة الأمنية في التعامل مع كل الشائعات، حيث يختلف الأسلوب طبقا لكل حالة، فيجب أن يتراوح ما بين الإسراع في تكذيبها، أو تجاهلها، أو التشكيك في مصدرها، أو تحويل الأنظار عنها، أو إطلاق شائعة مضادة.

التجربة الإمارتية:

١- **حذّرت وزارة الداخلية الإماراتية** أفراد الجمهور من تداول الشائعات أو أي معلومات لم تصدر عن الجهات المعنية الرسمية، بشأن فيروس «كورونا المستجد»، داعية إلى ضرورة تحري الدقة واتباع الإجراءات الوقائية الصادرة عن وزارة الصحة ووقاية المجتمع والهيئات الصحية في الدولة، وأكدت أنها تشدّد إجراءاتها في ملاحقة مروجي الشائعات والأكاذيب بشأن حالات فيروس كورونا داخل الدولة، وتقديمهم للعدالة، محذّرة الأفراد من تعرضهم للمساءلة القانونية في حال مشاركتهم في ترويج هذه الشائعات، وتصدت جهات حكومية وصحية وتعليمية عدة، ونفي عدد كبير من الشائعات والأخبار المفبركة التي تم ترويجها بشأن اكتشاف حالات الإصابة بفيروس «كورونا» داخل الدولة، بهدف بث الفزع والهلع في نفوس أفراد المجتمع.

٢- نجحت الإدارة العامة للتحريات والمباحث الجنائية في شرطة دبي، في تحقيق مؤشر صفر% في بلاغات جرائم «الديب فيك» أو التزييف العميق التي انتشرت أخيراً في بعض الدول. وهذه التقنية تتلاعب بالبرمجيات لتشكيل مجموعة صور ومقاطع فيديو مزيّفة لشخص ما بطريقة احترافية[٧٦].

---

[٧٦] نقلاً عن سوميه سعد، جريدة الخليج الإماراتية، لا بلاغات عن جرائم «التزييف العميق» في شرطة دبي، بتاريخ ٢ أكتوبر ٢٠٢٢ ومتاح علي:
https://www.alkhaleej.ae/2022-10-02/

(ISSN: 2537- 0758)

٣- كما حذرت وزارة الداخلية الإماراتية الجمهور من تداول الإشاعات والأخبار الكاذبة، التي تستهدف أمن واستقرار المجتمعات، وطالبت بعدم نشر أي أخبار على مواقع التواصل ما لم تكن من مصادرها الأساسية. ودعت إلى الابتعاد عن نقل الشائعات وعدم القيام بنشر معلومات وأفكار غير صحيحة ونسبتها إلى آخرين، وعدم نشر وتداول أي تعليقات أو معلومات والتعرض والمساس بالأعراض وانتهاك خصوصية الأفراد والعائلات، مؤكدةً أن الجهات المختصة توفر المعلومات عبر وسائل الإعلام ووسائل التواصل الاجتماعي وبكل الطرق المتاحة. وأوضحت، أن إطلاق الشائعات وترويج الصور ومقاطع الفيديو السلبية عبر مواقع التواصل الاجتماعي تعرض أصحابها للمساءلة القانونية، وأن هناك مسؤولية قانونية مترتبة على هذه الأفعال، يعاقب عليها قانونا العقوبات وتقنية المعلومات.

٤- إن الشرطة الإماراتية تعمل باحتراف لتوحيد وتكثيف الجهود الأمنية، في مكافحة كل أشكال الجريمة، ومنها الإلكترونية وتسعي لضبطها بدوريات إلكترونية تتولى الرصد، وضبط المتورطين، ووضع خطط واستراتيجيات مدعومة بأنظمة الذكاء الاصطناعى، تعزز الأمن وتمنع وقوع الجريمة.

خامساً- رؤية لتعزيز العلاقة بين جهاز الإعلام الأمني ووسائل الإعلام الأخرى، وما يتطلب ذلك من القيام بالآتي:

- حرص جهاز الإعلام الأمني على تقديم المعلومات الصحيحة سريعا لأجهزة الإعلام الأخرى، نظرا لحاجة هذه الأجهزة إلى الوصول للحقيقة في أسرع وقت ممكن.
- تنمية الحس الأمني لدى المواطن، لتحصينه ضد خطر شائعات الإنترنت، وذلك من خلال إشراكه في المنظومة الأمنية، كي يعي أهمية دوره في الحفاظ على الأمن، وذلك عن طريق توسيع نطاق الحوار بالنسبة للسياسات الأمنية، وغزالة المفاهيم المغلوطة والسلبية المُتواجدة في أذهان بعض المواطنين عن علاقتهم بالجهاز الأمني.
- التواصل الدائم مع المؤسسات الرسمية والمُجتمعية الأخرى ذات الصلة بعمل جهاز الإعلام الأمني، فلا يمكن أن ينجح الإعلام والأمني في تحقيق مقاصده

المرجوة، إلا حين أن تتكامل جهوده مع كافة المؤسسات الإعلامية، والاجتماعية، والتربوية الأخرى.

- تتبعُ مصدر الشائعة، الكشف عن مروجيها، والتنبيه لمخاطرها ونشر الحقائق والأرقام المُتصلة بها، لبيان زيفها.
- استخدام نظام "كشف الكذب الإلكتروني" الذي ظهر حديثاً، ويهدف إلى التأكد من صحة الشائعة التي تنقل على مواقع الإنترنت، حيث تقوم آليه عمله على تحليل البيانات، لمعرفة مدى صدق البيانات المنشورة على مواقع التواصل الاجتماعي كما في رسائل موقع "تويتر"، والتعليقات العامة على موقع "الفيس بوك"، والمُنتديات العامة، يحدد النظام ما إذا كانت حسابات مواقع الاجتماعي المُستخدمة في نشر الشائعة قد أنشئت خصيصاً لهذا الغرض[٧٧].

وتُعد الأجهزة الأمنية من أهم أجهزة الدولة المنوطة بها حفظ الأمن داخل المُجتمع، ويقع عليها العبء الأكبر في تحقيقه[٧٨]، أن الدولة بذلت كثيرا من الجهود التي تهدف إلى محاربة ومجابهة حروب الجيل الرابع والخامس على كافة الأصعدة، وتضمنت الاستراتيجية المصرية عددا من النقاط والمحاور الرئيسية في هذا الصدد، كان من أبرزها الاستثمار في العنصر البشري في مجالات تطوير البرمجيات ونظم الحماية، والعمل على مشروع وطني لأجل حماية البنية المعلوماتية التحتية من الاختراق، وتفعيل استراتيجية الأمن السيبراني في شكل استراتيجية قومية لمواجهة الخطر، والعمل على رفع الوعي المجتمعي لما نواجه من حروب سيبرانية[٧٩].

---

[٧٧] سامر جمال، المردود الأمني للشائعات ودور الشرطة في مواجهتها، المرجع السابق، ص٢٧١.

[٧٨] احمد على الخضري، دور المتحدث الرسمي لوزارة الداخلية وانعكاساتها على الأداء الأمني، رسالة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، القاهرة، ٢٠٢٠، ص٢٥.

[٧٩] أيمان رجب، سياسات مكافحة الإرهاب في مصر، مركز الدراسات السياسية والإستراتيجية، مرجع سابق، ص٩.

تقرير إنجازات وجهود وزارة الداخلية عن عام ٢٠٢١"، الصفحة الرسمية لوزارة الداخلية على الفيس بوك، ٢٠٢٢/١/٢٣ https://www.facebook.com/MoiEgy (تاريخ الاطلاع ٢٠٢٢/١/٢٣).

(ISSN: 2537- 0758)

الخاتمة

إن تقنية التزييف العميق ستصبح شائعةً في النهاية، ويمكن استخدامها كسلاح سياسي، وقد يأتي يوم نفقد فيه الثقة بكل مقاطع الفيديو المنشورة على الإنترنت والتلفزيون، لكن العالم مستمر بتطوير التقنيات المضادة لها، في محاولة لمكافحة التزييف العميق؛ أخطر تهديد لجرائم الذكاء الاصطناعي، إن الأمر يتطلب مزيجًا من الدفاع التكنولوجي والمسؤولية والوعي البشري لمكافحة هذا الطوفان الجديد من الأخبار المزيفة، التي تهدد نسيج المجتمعات، ويجب أن يتم تعميم وتوعية المواطنين في كل مناسبة بمخاطر وسبل التصدي للتزييف العميق بالطريقة نفسها التي يتم بها التعامل مع مخاطر برامج الفدية أو خرق البيانات فيما سيعد خطوة أولى نحو مكافحة المعلومات المضللة وحماية الأسر والمجتمعات.

النتائج

- ان مخاطر وسائل التواصل الاجتماعي على أمن المجتمعات قد يصل إلى انتشار العنف الداخلي، حيث يمكن عبر وسائل التواصل الاجتماعي نشر ثقافات وتوجهات وأفكار لا تنسجم مع قيم المجتمع من خلال تقنية التززيف العميق.
- مع التزايد الملحوظ في معدلات الاستخدام أصبحت المنصات الإلكترونية أداة خصبة لترويج الشائعات والأخبار المزيفة والكاذبة؛ لذا فالشائعات تعد إحدى أدوات الحروب الحديثة، وتندرج ضمن ما يسمى الجيل الخامس من الحروب.
- يستخدم الذكاء الاصطناعي كأداة من أدوات الحرب النفسية في الواقع المعاصر، من خلال ما يعرف بـ "التزييف العميق" الذي يمكن أن يتم من خلاله تخليق صورة إنسان استناداً إلى خوارزميات الذكاء الاصطناعي، وأكدت دار الافتاء أنه لا يجوز شرعًا استخدام **تقنية (Deepfake: التزييف العميق)** لتَلْفِيق مقاطع مَرْئية أو مسموعة للأشخاص باستخدام الذكاء الاصطناعي لإظهارهم يفعلون أو يقولون شيئًا لم يفعلوه ولم يقولوه في الحقيقة.
- دخلت التكنولوجيا بالاعتماد على قوة الذكاء الاصطناعي في هذا المجال لأداء وظيفة كشف النصوص والعبارات والمحتويات المزيفة وتطوير الأداة، عن

طريق معالجة اللغة الطبيعية لفهم النص وتحليله، حيث تتحقق الخوارزميات من مصداقية محتوى ما استنادًا إلى مقارنته بمحتويات كثيرة مماثلة.

- يتم استخدامها البلوك تشين في تشفير البيانات والمعلومات والصور– من الأخبار الرسمية الموثوقة الصادرة من جهات الدولة الرسمية والإعلامية والجريدة الحكومية ومواقع الرسمية للحكومات على صفحات التواصل الاجتماعي– وذلك لعدم تركها عرضة في أيدي الدول والمنظمات المعادية للدولة– للعبث بها وتزييفها من تغير محتوها او زمن صدورها.

التوصيات

- ضرورة تعزيز آليات التقييم الدقيق للمحتوى المنشور عبر مواقع التواصل الاجتماعي، بما يضمن دراسة الرأي العام، واكتشاف المصطلحات المُشفرة، والتي تهدف إلى نشر الكراهية، وذلك من خلال دمج الذكاء الاصطناعي مع العامل البشري الذي يتسم بالمهارة للكشف عن المحتويات المسيئة، مع توفير آليات تتضمَّن اللهجات واللغات المحلية المختلفة، والتي قد تُستَخْدم في إرسال رسائل مُشفرة تحُض على الكراهية.
- تدريب النشء والشباب في على كيفية الاستخدام الآمن لمواقع التواصل الاجتماعي من خلال دورات متخصصة يشرف عليها الخبراء والمتخصصون الوطنيون، وتنمية الوعي لديهم بخطورة الفكر الذي تبثه الجماعات المتطرفة والإرهابية على هذه المواقع.
- دعوة وسائل الإعلام المختلفة إلى تأهيل كوادرها وتدريبهم على سبل التحقق من الأخبار والمصادر الإلكترونية والقدرة على التحليل الرقمي بكل أشكاله وإيجاد آليات لدعم الصفحات والحسابات والمواقع التي تهدف إلى كشف الشائعات، وهذا يتم خلال عمليات التنمية الشاملة ومحاربة الإرهاب والتطلع نحو مستقبل أفضل للوطن العربي
- الاستعانة بتقنية التعاملات الرقمية (بلوك تشين) في تنفيذ المعاملات الحكومية داخل مؤسسات الدولة لأنها على الحفاظ على قوائم مقاومة للتلاعب في سجلات البيانات المتنامية باستمرار "والصور والنصوص والعبارات والبيانات

(ISSN: 2537- 0758)

الرسمية، وتتيح تبادلاً آمنا للمواد القيّمة كالأموال أو الأسهم أو حقوق الوصول إلى البيانات

- ضرورة تطوير مصنفات وتطبيقات التعلم العميق، التي يمكنها توظيف الذكاء الاصطناعي لفحص لمقاطع الفيديو الأولية للإشارة إلى مدى أصالتها عبر العلامات المائية للفيديو البيومتري.
- يجب عودة التوعية الأسرية والمجتمعية والإعلامية، لمواجهة شراسة الحروب الإلكترونية وخاصة التزييف العميق والفيديوهات والأخبار المفبركة التي تستهدف شباب وأبناء الوطن عبر وسائل التواصل الاجتماعى بشكل مباشر وغير مباشر" بهذه الكلمات عبر عدد كبير من الخبراء الأمنيين، عن حقيقة الوجه الأخر لوسائل التواصل الاجتماعى، وكشف حقيقة ما يدار ويُشن نحو الشباب.
- توظيف وسائل التواصل الاجتماعي في التصدي للأيديولوجيات المتطرفة والأفكار الهدامة التي تستهدف النشء والشباب، وهناك العديد من التجارب المهمة التي يمكن الاستفادة منها في هذا الشأن، كتجربة "مركز صواب"، الذي تم تأسيسه بالتعاون بين دولة الإمارات العربية المتحدة والولايات المتحدة الأمريكية في عام ٢٠١٥، بهدف التصدي للأفكار المغلوطة وتصويبها عبر وسائل التواصل الاجتماعي، وإتاحة مجال أوسع لإسماع الأصوات المعتدلة لأُولئك الذين يرفضون الأفكار المتطرفة والأعمال الإرهابية ويقفون ضد الأفكار المنحرفة التي يروجها أتباع الضلال.

قائمة المراجع

أولاً- المراجع باللغة العربية:

١- الكتب والمؤلفات:

١- أمينة خيري: - التزييف عميق والتضليل شديد في عصر التمكين الرقمي، موسوعة "Independent Arabia"، بتاريخ ١٥ يوليو ٢٠٢٢.

٢- ايمان رحب: - الفاعلية والتحديات".. سياسات مكافحة الإرهاب، المركز العربي للبحوث، القاهرة، ٢٠١٩.

٣- إيهاب خليفة: - الحرب السيبرانية، الاستعداد لقيادة المعارك العسكرية في الميدان الخامس، دار العربي للنشر والتوزيع، القاهرة، ٢٠٢١.

٤- رغدة البهي: - الخداع العميق: تحديات أمنية وإشكاليات حقيقية، المركز المصري للفكر والدراسات الاستراتيجية (ESCC)، وحدة الأمن السيبراني، نشر بتاريخ ٢٧ مارس ٢٠٢١.

٥- عمار ياسر البابلي: - الذكاء الاصطناعى في مواجهة الشائعات وجرائم تمويل الإرهاب في البيئة السيبرانية "التداعيات وسبل المواجهة"، المنظمة العربية للتنمية الإدارية، جامعة الدول العربية، القاهرة، ٢٠٢٣.

٦- كلاوس شواب: - الثورة الصناعية الرابعة، ملخصات مؤسسة محمد بن زايد للمعرفة، دبي، الإمارات، ٢٠٢٠.

٧- محمد بكراه: - إستراتيجية المركز الأوروبي للجريمة الإلكترونية في مكافحة الجريمة السيبرانية، كلية الحقوق والعلوم السياسية- جامعة جيلالي ليابس- سيدي بلعباس- الجزائر، ٢٠٢٠.

(ISSN: 2537- 0758)

٨- هشـــام الـــزوام: - تقنية التزييف العميق بين الفوائد والأضرار.. وطرق الاكتشاف، بوابة الاقتصاد الرقمي الأولي، بتاريخ، ١١ يناير، ٢٠٢٢.

٢- رسائل الدكتوراه والماجستير:

١- احمد على الخضري دور المتحدث الرسمي لوزارة الداخلية وانعكاساتها على الأداء الأمني، رسالة دكتوراه، كلية الدراسات العليا، أكاديمية الشرطة، القاهرة، ٢٠٢٠.

٢- سماح بن ابراهيم استخدام تقنية الذكاء الاصطناعي (التزييف العميق) في الفبركة الإعلامية دراسة تحليلية لعينة من الفيديوهات المنشورة على منصة تويتر الانتخابات الرئاسية الأمريكية لسنة ٢٠٢٠ نموذجا، رسالة ماجستير، جامعة قاصدي مرباح، الجزائر، ٢٠٢٠.

٣- سامر جمال المردود الأمني للشائعات ودور الشرطة في مواجهتها، دراسة تطبيقية على الإنترنت، رسالة دكتوراه، أكاديمية الشرطة، كلية الدراسات العليا، القاهرة، ٢٠٢١.

٣- الأبحاث العلمية والدراسات:

١- إيهاب خليفة: فرص وتهديدات الذكاء الاصطناعي في السنوات العشر القادمة، تقرير المستقبل: مجلة اتجاهات الأحداث، ابوظبي، الامارات العدد ٢٧، ٢٠١٨

٢- رامى متولي القاضي: - تم نشرها فى مركز الدراسات العربية، القاهرة ٢٠٢٠.

٣- سالي يوسف: كيف نواجه استخدام الذكاء الاصطناعي في التضليل المعلوماتي، دراسات، مركز المستقبل

للأبحاث والدراسات المتقدمة لا يجوز استخدام تقنية "Deep Fake" لتزييف الفيديوهات، إدارة الفتوي بدار الإفتاء المصري، القاهرة، نشر في ٦ يناير ٢٠٢٢، http://www.dar-alifta.gov.eg/home/index

٤- عمار ياسر البابلي تطبيقات الذكاء الاصطناعي في العمل الأمني، مجلة الأمن والقانون، علمية محكمة، أكاديمية شرطة دبي، العدد (١)، يناير ٢٠٢١.

٥- معين الميتمي: "التزييف العميق".. مستقبل القوانين المنظمة للبرمجيات الذكية، تقرير جريدة العين الإماراتية الإخبارية، بتاريخ ١٣ مارس ٢٠٢١ ومتاح على: https://al-ain.com/article/deefacke-the-future-of-smart-software-laws

٦- تقرير شركة كاسبرسكي المتخصصة في أمن وسلامة المعلومات عن مخاطر الأمن والخصوصية ذات الصلة بالواقع المعزز والواقع الافتراضي،

٧- تقرير فيسبوك... الذكاء الاصطناعي لمحاربة الأخبار الزائفة ، مجلة (W.D) الدولية ومتاح على: https://p.dw.com/p/34xGP (تاريخ الزيارة ٢٠٢٢/١/٢٩).

٨- دار الافتاء: لا يجوز استخدام تقنية " Deep Fake" لتزييف الفيديوهات، إدارة الفتوي بدار الإفتاء المصري، القاهرة، نشر في ٦ يناير ٢٠٢٢، http://www.dar-alifta.gov.eg/home/index

(ISSN: 2537- 0758)

٤- المجلات والمقالات والتقارير:

١- أحمد حازم مصطفي: – مقال "تقنية المعلومات"، حكومة دبي، هيئة المعرفة والتنمية البشرية، ٢٠١٥.

٢- بن عودة حسكر مراد: إشكالية تطبيق أحكام المسؤولية الجنائية على جرائم الذكاء الاصطناعي، مجلة الحقوق والعلوم الإنسانية، جامعة تلمسان، الجزائر المجلد ١٥ / العدد: ٠١– ٢٠٢٢.

٣- أحمد عبدالموجود أبوالحمد زكير: جريمة التزييف الإباحي العميق (دراسة مقارنة)، المجلة القانونية (مجلة متخصصة في الدراسات والبحوث القانونية) مجلة علمية محكمة، جامعة قانون الوادي، ٢٠٢٢.

٤- احمد مصطفى معوض: استخدام الذكاء الاصطناعي–تقنية التزييف العميق deep fake في قذف الغير نموذجا دراسة فقهية مقارنة معاصرة، مجلة البحوث الفقهية والقانونية، جامعة الأزهر، العدد ٣٩، أكتوبر ٢٠٢٢.

٥- مصطفى صلاح عبد الحميد: التزييف الرقمي وأثره على حجية الأدلة الرقمية في الدعاوي الجنائية دراسة فقهية مقارنة، مجلة الفقه المقارن، كلية الشريعة القانون، جامعة الأزهر، القاهرة، المقالة ١٤، المجلد ٤٠، العدد ٤٠، أكتوبر ٢٠٢٢.

٦- محمود سلامة عبد المنعم الشريف: جريمة الانتقام الإباحي عبر تقنية التزييف العميق" Deepfakes" والمسؤولية الجنائية عنها، مجلة كلية الحقوق، جامعة الإسكندرية،

المقالة ٥، المجلد ٢.٢٠٢٢، العدد ١، يوليو ٢٠٢٢.

٧- عمار ياسر البابلي، المخاطر الأمنية للتزييف العميق وآليات المواجهة، مجلة الفكر الشرطي، مركز بحوث شرطة الشارقة بالإمارات العربية المتحدة عدد اكتوبر– العدد ١٢٧– أكتوبر ٢٠٢٣

٨- عمار ياسر البابلي دور الذكاء الاصطناعي في مواجهة الظواهر الإجرامية المُستحدثة عبر طبقات الإنترنت، مجلة الدراسات الأمنية والقانونية، أكاديمية شرطة قطر، عدد الثانى أكتوبر ٢٠٢٤

٩- منة الله كمال موسى ديـــــــــــاب: سلوك حماية الخصوصية الرقمية البيومترية لدى مستخدمي تطبيقات التزييف الْعميق من طلبة الجامعات المصرية، المجلة العربية لبحوث الإعلام والاتصال، كلية الإعلام بالجامعة الكندية بالقاهرة، العدد ٣٧– أبريل/ يونيو– ٢.

١٠- سامح محمد الشريف: تحليل البيانات الضخمة في تحليل مواقع التواصل الاجتماعي، مجلة رؤي استراتيجية، علمية محكمة، المجلد السابع، العدد (١٩)، يونيو ٢٠٢٠.

١١- نايلـــة الصـــليبي: إنتل تطور أداة جديدة لكشف التزييف العميق ومحاربة التضليل، مجلة علمية مونت كارلو الدولية (MCD)، نشر في ٢٠٢٢/١١/٢٤.

١٢- المنتدى الاقتصادي العالمي ٢٠٢٣ دافوس٢٠٢٣ المقام في دولة سويسرا التقرير متاح علي

(ISSN: 2537- 0758)

https://www.swissinfo.ch/ara

١٣- تقرير الذكاء الاصطناعي ومخاطر التزييف العميق: تقرير الذكاء الاصطناعي ومخاطر التزييف العميق، توجهات عالمية، مركز المعلومات واتخاذ القرار، رئاسة مجلس الوزراء المصري، بتاريخ ٢٥ مايو ٢٠٢٣ ومتاح على: https://www.idsc.gov.eg/DocumentLibrary/LandingPage

٥- **القوانين والمواد القانونية**:

١- قانون رقم ١٧٥ لسنة ٢٠١٨ بشأن بمكافحة جرائم تقنية المعلومات، الجريدة الرسمية، القاهرة، نشر بتاريخ ١٤- ٠٨- ٢٠١٨.

٢- مرسوم بقانون اتحادي رقم (٣٤) لسنة ٢٠٢١ في شأن مكافحة الشائعات والجرائم الإلكترونية

٣- المواد (٦) و(١٩) و(٢٠) من قانون الأمن السيبرانى الصينى ٢٠١٦م.

٤- المادة (٧) من قانون حماية الأمن السيبرانى الأوكرانى ٢٠١٧م.

ثانياً- المراجع باللغة الأجنبية:

- Yang, Y. Li and S. Lyu, "Exposing Deep Fakes Using Inconsistent Head Poses," ICASSP 2019- 2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2019
- Dayani، Raveena، Nikita Chhabra، Tarina Kadina، and Rishabh Kaushal. (2015). “Rumor Detection in Twitter: An Analysis in Retrospect.” In 2015 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)
- Vaccari, Cristian, and Andrew Chadwick, “Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News,” social media + Society, Vol. 6, No. 1, January 2020

- **Atlantic Council's Digital Forensic Research Lab, "#Stop the Steal: Timeline of Social Media and Extremist Activities Leading to 1/6 Insurrection," Just Security, February 10, 2021.**
- **SOURCE: Tom [@deeptomcruise], "Sports!" 2021.**
- **NOTE: As of April 12, 2022, this TikTok video had more than 16.1 million views.**
- **Victor, Daniel, "Your Loved Ones, and Eerie Tom Cruise Videos, Reanimate Unease with Deepfakes," New York Times, March 10, 2021**
- **Rushing, Ellie, "A Philly Lawyer Nearly Wired $9,000 to a Stranger Impersonating His Son's Voice, Showing Just How Smart Scammers Are Getting," Philadelphia Enquirer, March 9, 2020.**
- **Chawki, M.: Cybercrime in France: an overview. Computer Crime Research Center. December 2005. Downloaded January 23rd, 2006, from: http://www.crime-research.org/articles/cybercrime-in-france-overview/ (2005) www.scopus.com.**
- **ITU (2018). Global Cybersecurity Index 2018. Geneva. Studies & Research**
- **Triplett, William J. 2022. "Addressing Human Factors in Cybersecurity Leadership" Journal of Cybersecurity and Privacy 2, no. 3: 573-586. https://doi.org/10.3390/jcp2030029 www.scopus.com**
- **Tu, C.Z.; Yuan, Y.; Archer, N.; Connelly, C.E. Strategic value alignment for information security management: A critical success factor analysis. Inf. Comput. Secur. 2018, 26, 150–170. www.scopus.com**
- **Von Solms, R., & Van Niekerk, J. (2013). From information security to cyber security. Computers and**

(ISSN: 2537- 0758)

Security, 38, 97 www.scopus.com

- Pósa, Tibor, and Jens Grossklags. 2022. "Work Experience as a Factor in Cyber-Security Risk Awareness: A Survey Study with University Students" Journal of Cybersecurity and Privacy 2, no. 3: 490-515. https://doi.org/10.3390/jcp2030025 www.scopus.com
- Cheng, Eric C. K., and Tianchong Wang. 2022. "Institutional Strategies for Cybersecurity in Higher Education Institutions" Information 13, no. 4: 192. https://doi.org/10.3390/info13040192 www.scopus.com
- ttps://www.forbes.com/sites/louiscolumbus/2018/01/12/10-charts-that-will-change-your-perspective-on-artificial-intelligences-growth/#704da34a4758
- Sayler, Kelley M., and Laurie A. Harris, “Deep Fakes and National Security,” Congressional Research Service, updated June 8, 2021.
- A. Ferrer, Cristian Canton, Ben Pflaum, Jacqueline Pan, Brian Dolhansky, Joanna Bitton, and Jikuo Lu, “Deepfake Detection Challenge Results: An Open Initiative to Advance AI,” Meta AI, blog, June 12, 2020. As of October 10, 2021
- A. Dhiran, D. Kumar, Abhishek, and A. Arora, "Video Fraud Detection using Blockchain," 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), 2020
- Tech , Blockchain Based Approach for tackling Deepfake videos, International Journal of Scientific Research in Computer Science, Engineering and Information Technology
- ISSN: 2456-3307 (www.ijsrcseit.com) doi: https://doi.org/10.32628/CSEIT217372

- **Eling, M.; Wirfs, J. What are the actual costs of cyber risk events? Eur. J. Oper. Res. 2019, 272, 1109–1119. www.scopus.com**

ثالثاً ـ المواقع الإلكترونية:

- **https://me.kaspersky.com/resource-center/threats/security-and-privacy-risks-of-ar-and-vr**
- **DIGITAL 2021: GLOBAL OVERVIEW REPORT ON: https://datareportal.com/**
- **https://www.internetworldstats.com/stats5.htm**
- **دليل التزييف العميق، البرنامج الوطنى للذكاء الاصطناعى، يوليو ٢٠٢١، الامارات العربية المتحدة ومتاح علي:**
- **https://ai.gov.ae/wp-content/uploads/٠٧/٢٠٢١/AI-DeepFake-Guide-AR-٢٠٢١.pdf**
- **Jakub Przetacznik with Simona Tarpov, Russia's war on Ukraine: Timeline of cyber-attacks, European Parliamentary Research Service, June 2022, on https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_EN.pdf**
- **Destructive malware targeting Ukrainian organizations, Microsoft, January 15, 2022, on https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/.**
- **Meenu EG, "Try These 10 Amazingly Real Deepfake Apps and Websites," webpage, Analytics Insight, May 19, 2021. As of October 10, 2021: https://www.analyticsinsight.net/try-these-10-amazingly-real-deepfake- apps-and-websites/**
- **Changsha Shenduronghe Network Technology, ZAO, mobile app, Zao App APK, September 1, 2019. As of October 10, 2021: https://zaodownload.com**

(ISSN: 2537- 0758)

- **TODD C. HELMUS, Artificial Intelligence, Deepfakes, and Disinformation, Perspective**
- **EXPERT INSIGHTS ON A TIMELY POLICY ISSUE, The RAND Corporation, July 2022 at:**
- **https://www.rand.org/pubs/perspectives/PEA1043-1.html**
- **Linvill, Darren, and Patrick Warren, "Understanding the Pro-China Propaganda and Disinformation Tool Set in Xinjiang," Lawfare Blog, December 1, 2021. As of June 6, 2022: https://www.lawfareblog.com/understanding-pro-china-propaganda- and-disinformation-tool-set-xinjiang**
- **https://datareportal.com/essential-instagram-stats**