DISCUSSION PAPER

The Deepfake Menace: Legal Challenges in the Age of AI

Şeymanur Yönt

TRT WORLD research centre

DISCUSSION PAPER

The Deepfake Menace: Legal Challenges in the Age of AI

Şeymanur Yönt

TRT WORLD research centre

WRITTEN BY

Şeymanur Yönt

PUBLISHER

TRT TRAINING AND RESEARCH DEPARTMENT

March 2024

TRT TRAINING AND RESEARCH DEPARTMENT

AHMET ADNAN SAYGUN STREET NO:83 34347

ULUS, BEŞİKTAŞ

İSTANBUL / TÜRKİYE

TRT WORLD LONDON

PORTLAND HOUSE

4 GREAT PORTLAND STREET NO:4

LONDON / UNITED KINGDOM

TRT WORLD WASHINGTON D.C.

1819 L STREET NW SUITE 700 20036

WASHINGTON DC

researchcentre.trtworld.com

Introduction

Seeing is no longer believing!

Technology has advanced in ways that blur the lines between what is true and what is simulated. Deepfakes, being part of that technology, is a miracle for those of us who once marvelled at face-swapping and photoshopping. Deepfakes use artificial intelligence, which makes it possible to create videos, photos, and audio that are difficult for humans to recognise as phoney. This poses serious risks, with potential consequences ranging from unfair election practices to the use of falsified evidence in court. Therefore, prompt legal action is necessary as deepfake technology continues to proliferate and evolve rapidly.

Addressing the risks around deepfakes is more important than ever. Because 2024 is set to be the biggest global election year in history. This technology may easily influence public opinion and lead to unfair election practices. On the other hand, even a world star like Taylor Swift had to act against the widespread dissemination of her deepfaked pornography all over the Internet.

Existing laws, primarily at the national level, such as criminal statutes and data protection regulations, aim to mitigate the risks associated with deepfakes. However, these laws are inadequate in addressing the multifaceted challenges posed by deepfakes, highlighting the urgent need for stronger legislation.

This discussion paper outlines the dangers posed by deepfakes, examines the adequacy of current legal frameworks in addressing these risks, and proposes strategies for overcoming legal challenges associated with deepfake technology.

Taylor Swift. (Mintaha Neslihan Eroğlu - Anadolu Agency)

Pros and Cons

Deepfakes can be fun and artistic. Some afficionados created a deepfake mock-up of Jerry Seinfeld in the Pulp Fiction movie (Nealy, 2023). Others let Salvador Dali greet museum visitors (Aouf, 2019). Deepfakes have many pros, such as saving time and labour in the film industry, educating people in more interactive ways, and interacting with deceased characters. For example, during the filming of The Last Jedi, after Carrie Fisher passed away suddenly, filmmakers staged extra conversations utilising clips from actual recordings (Narcisse, 2017). Deepfake technology can also allow, for instance, a person who has lost the ability to speak because of illness, to retrieve his own voice rather than use a computerised version (Shakeri, 2018).

Deepfakes also pose a significant threat with far-reaching consequences. They can manipulate the truth so easily that the quick dissemination of misinformation will become inevitable. As David Doermann, the director of the Artificial Intelligence Institute at the University of Buffalo, states, "A lie can go halfway around the world before the truth can get its shoes on" (Galston, 2020).

Deepfakes become especially problematic for content that is subtle and not too obvious to detect for non-professional crowds. For example, a significant portion of the audience mistook the witty yet fabricated speech of the Belgian prime minister as true. The speech, disseminated by a political faction in Belgium, depicted the Belgian prime minister delivering a speech associating the COVID-19 pandemic with environmental degradation and advocating for urgent measures to address climate change (Galindo, 2020). While it may be considered beneficial to circulate such subtle content to draw attention to climate change, carefully crafted content can do greater harm, especially when it deals with controversial issues.

At the individual and organisational levels, deepfakes enable wicked activities such as financial exploitation through the misuse of someone else's identity, the production of non-consensual pornography leading to severe reputational damage, fraudulent endorsements of products or individuals, and smearing a competitor's business reputation. The proliferation of non-consensual deepfake pornography is particularly a threat, as a study in 2019 found that revenge pornography videos account for 96% of all deepfake videos (Durbin & Graham, 2024). The swift proliferation of Taylor Swift's deepfake pornography to millions of views on X within a short period in January 2024, coupled with the accessibility of the shared post for 17 hours, is evidence of the seriousness of the danger (Weatherbad, 2024).

At the societal level, the proliferation of deepfake technology exacerbates the spread of misinformation by allowing for the fabrication of convincingly realistic videos and audio clips, which can be disseminated widely across various online platforms. With deepfakes, public figures can be falsely depicted engaging in actions they've never committed, such as accepting bribes, expressing racist sentiments, making diplomatically sensitive statements, or perpetrating violence against civilians. The fabrication of a video depicting Obama referring to Trump as a "dipshit" serves as a notable example of this phenomenon, fuelling confusion, undermining public trust, and exacerbating polarisation (Vincent, 2018).

Deepfakes also pose a significant risk to the integrity of democratic processes, as they enable the creation of deceptive content designed to mislead voters, manipulate public perceptions of candidates, and ultimately undermine the fairness and legitimacy of elections. This situation opens the floodgates for manipulation and propaganda, often perpetrated by opponents and even foreign entities. During the French elections in 2017, Macron's campaign was the victim of cyberattacks attributed to a Russian-backed hacker group (Geller & Vinocur, 2017). The UK Home Secretary James Cleverly warned against Russia and Iran-backed deepfakes that endeavour to manipulate the democratic processes (Ambrose, 2024). The involvement of foreign entities shows that such attacks not only threaten the integrity of elections but also have profound national security implications.

The emergence of deepfake technology also raises concerns regarding the admissibility of evidence in legal proceedings, as the ability to fabricate convincing audio-visual material undermines the reliability of such evidence, potentially leading to miscarriages of justice and undermining the rule of law. Finally, the widespread prevalence of deepfakes threatens to erode public trust in the authenticity of information, as individuals may become increasingly sceptical of visual and auditory evidence, undermining the foundation of discourse and decision-making in society.

Legal Solutions

Considering the threat posed by deepfakes, issuing an adequate legislation is becoming increasingly urgent. On October 2023, President Joe Biden issued an executive order aimed at managing the risks of AI, calling for protections against AI-enabled fraud and deception and for protecting privacy (The White House, 2023).

Some laws are already in place, such as criminal laws, whereas some laws are yet to be enacted, especially those directly regulating the use of deepfakes. Overall, laws on deepfakes focus on three main issues: protecting privacy, protecting elections, and protecting creators. To that end, a broad scope of laws, including privacy laws, criminal laws, civil laws, cyber laws, and human rights laws, can be referred to against misuse of deepfakes. Moreover, governments are on track to enact AI or deepfake-specific laws.

2.1. Privacy Laws

Deepfakes present a significant threat to privacy. Privacy laws, while not directly purposed for deepfakes, provide a certain degree of protection against their misuse. The photos and videos used to create deepfakes often contain individuals' personal data. Processing such data requires the individual's explicit consent unless the processing falls within exceptions to consent outlined by law, such as the existence of a legitimate interest. Therefore, producing a politician's deepfake without a legitimate interest or explicit consent is a breach of privacy laws. Making someone's fake pornography does not fall under the exceptions, as there is no legitimate interest, and it requires explicit consent. Therefore, in cases of non-consensual pornographic production, privacy laws are violated as well, and those responsible for creating and distributing such deepfakes may face fines. Erasing or rectifying inaccurate personal data, including deepfakes, is also possible by law, as the European General Data Protection Regulation (**GDPR**) provides for it. The GDPR, as well as many other country's laws, also give the victims the right to exercise their right to be forgotten (European Parliament & Council of the European Union, 2016, Article 17) even if there is no inaccuracy, enabling them to request the erasure of personal data concerning them.

2.2. Criminal Laws

Criminal laws, especially those on privacy, pornography, fraud, and harassment, play a crucial role too in addressing the misuse of deepfakes. For instance, regarding personal data protection, Turkish law sets forth imprisonment for up to four years for individuals who unlawfully provide, distribute, or obtain another person's personal data (Turkish Criminal Code, 2004, Article 136). On the other hand, for deepfake pornography, laws on pornography may be utilised. For example, Section 163 of the Canadian Criminal Code mandates imprisonment for anyone who produces, distributes, or possesses child pornography, including content generated using deepfake technology (Canadian Criminal Code, 1985). The violation of privacy may also be applicable. For instance, the Turkish Criminal Code imposes imprisonment for individuals who disclose images or recordings of people's private lives (Turkish Criminal Code, 2004, Article 134/2). However, it is uncertain whether deepfake photos and videos fall under such laws as they are not really someone's images or recordings. Finally, there are also special legal regulations for offences committed on the Internet. For example, in Turkey, the law on the Regulation of Publications on the Internet and Combating Crimes Committed through Such Publications sets out the responsibilities of content providers and hosting providers and provides the possibility to block access to content when necessary.

2.3. Civil Laws

Civil laws are another option to impair the suffering resulting from deepfakes. As a result of the creation and dissemination of deepfakes, parties who suffer material or moral damage may have the right to compensation. For instance, in Quebec, if someone's privacy is violated via the use of their names, images, or voices for purposes other than legitimate public information, that person may claim remedy. In some legal systems, individuals affected by psychiatric illness or mental distress resulting from deepfake creation and dissemination may also have the right to seek legal remedies. However, proving that deepfakes cause psychiatric illness or mental suffering can be challenging.

2.4. Human Rights Laws

Human rights law provides a mechanism to address deepfakes, especially within the context of violations of an individual's right to privacy. Article 8 of the European Convention for Human Rights (ECHR) recognises everyone's right to have their private life respected. Case law of the European Court of Human Rights shows

that deepfakes as well may fall well under the rights protected by the ECHR. The case of Volodina v. Russia (no. 2) before the European Court of Human Rights is an example which concerned authorities' failure to protect the applicant against her partner, who created fake profiles and published intimate photos. Moreover, deepfake technology has the potential to perpetuate or exacerbate discriminatory practices by creating manipulated content that targets specific individuals or groups based on protected characteristics such as race, gender, or religion. Therefore, laws against discrimination may as well be referred to against deepfakes.

2.5. Copyright Laws

Existing copyright laws may prove effective against the misuse of deepfakes. These regulations address the issue of deepfakes to some extent, as deepfakes incorporating copyrighted material may face allegations of copyright infringement. Social media platforms may also be required to remove deepfakes that violate copyrights (Bass & Penning, 2023). International institutions also address the issues around deepfakes, questioning whether deepfakes should benefit from copyrights, to whom should own the copyright in a deepfake, and whether there should be a numeration for people whose likeness is used (Secretary of the World Intellectual Property Organization, 2020).

At this point, there is a debate about whether the fair use doctrine of the US laws or the fair dealing doctrine of the UK laws could justify the use of copyrighted content without permission. For example, in the US, depending on factors such as the purpose and character of the use, the nature of the original work, the amount and substantiality of the content borrowed, and the effect of such use on the potential market, the fair use doctrine may allow for the limited use of copyrighted material. More than that, deepfake itself can enjoy copyright protection, having a different purpose and nature than the original work. Existing copyright laws may lead to protecting misused deepfakes instead of protection against them. For this reason, existing copyright laws must be amended to address deepfakes in a more sophisticated manner.

2.6. Cybersecurity Laws

Cybersecurity laws and regulations, on the other hand, aim to protect digital systems and networks from unauthorised access, data breaches, and other cyber threats, including those involving deepfake technology. These laws may provide recourse to victims and may impose obligations on organisations to implement security measures to safeguard against deepfake-related cyberattacks and intrusions. The Anti-phishing Act of 2005 in the US, for instance, criminalises internet scams, imposing fines or imprisonment on individuals involved in fraudulently obtaining personal data (phishing). In the UK, on the other hand, the Computer Misuse Act of 1990 imposes fines or imprisonment for intention to commit cybercrime, which may involve the use of deepfakes for identity theft or fraud.

2.7. Consumer Protection Laws

Consumer protection laws aim to prevent deceptive practices that could harm consumers, including those involving deepfake technology. These laws may prohibit false advertising, deceptive marketing tactics, or the sale of fraudulent products or services created using deepfake technologies. For instance, in the US, courts have construed Section 43(a)(1)(A) of the Lanham Act to restrict the non-consensual use of an individual's "voice" and "persona" in a way that misleads customers into believing that the person endorses a certain commodity or service.

2.8. Defamation and False Light Laws

Defamation laws that aim to protect a person's reputation could help against misuse of deepfakes. If a deepfake harms someone's reputation, they can sue the person creating and sharing this material. For example, in Australia, altered photos were already the subject of a lawsuit. Therefore, deepfake photos or videos could also be sued over (Talas & Kearney, 2019). False light laws can also be utilised to address the misuse of deepfakes by targeting the emotional distress caused by the dissemination of deceptive content rather than solely focusing on the damage to reputation. By invoking false light laws, individuals affected by deepfake manipulation can seek legal remedies for the emotional harm inflicted by false portrayals. This approach complements defamation law and provides an additional avenue for holding perpetrators accountable for spreading malicious falsehoods through deepfake technology.

2.9. AI Specific Laws

Numerous AI-specific laws are either already in effect or in the process of being enacted to tackle issues surrounding deepfakes directly. Examples that deal with intimate visuals include the Defiance Act of 2024, which was introduced but has not yet been enacted in the US. The Defiance Act aims to "hold accountable those responsible for the proliferation of non-consensual, sexually explicit "Deepfake" images and videos, creating a civil remedy for

the victims (US Senate Committee on the Judiciary, 2024).

Similarly, the Assembly Bill 602 of California, already enacted, gives individuals the right to claim remedy against the creation and disclosure of sexually explicit materials related to themselves (An act to add Section 1708.86 to the Civil Code relating to privacy, 2019).

Other examples are the Intimate Images Protection Act and Images Protection Regulation of British Columbia, which give individuals the right to request deletion or destruction of all altered intimate images in a person's possession or control and to make such photos unavailable to others. They also provide for requesting damages and allow for applications on behalf of minors and the deceased (Catenacci, 2024).

The UK Online Safety Act, on the other hand, prohibits the sharing of manipulated explicit images or videos. However, the law does not prohibit the creation of pornographic deepfakes. The UK Online Harms Bill similarly prohibits sharing deepfake pornography.

There are also AI-specific laws that protect elections. For instance, deepfake videos that are produced with the intention of harming a candidate or influencing election results and are released within 30 days of an election are prohibited by Texas Senate Bill 751, with a modification to the state's election code (Artz, 2019). Additionally, Democrats in Hawaii, South Dakota, Massachusetts, Oklahoma, and Nebraska, as well as Republicans in Indiana and Wyoming, proposed legislation that would forbid media produced with AI support from being released within specific timeframes prior to elections unless a disclosure statement is included (Edelman, 2024).

Related to copyright laws, the No AI FRAUD Act, proposed in January 2024, aims to establish "a federal framework to protect Americans' individual right to their likeness and voice against AI-generated fakes and forgeries" (Sarnoff, 2024). The basis of the proposal is the individual's intellectual property rights in their likeness, i.e. a person's image or distinguishing features and properties, to be protected both during life and after death. If deepfake content is created and distributed in violation of this, the injured party will be compensated for the breach by paying a certain amount or by compensating for the damages suffered by the injured party. The No FAKES Act of 2023 similarly prohibits reproductions of human likeness (both visual and sonic), their distribution and transmission, and penalises platforms that publish such non-consensually generated content (NO FAKES Act of 2023, 2023). Recently, the Chinese government also passed stringent laws known as the Deep Synthesis Provisions, which forbid the production of deepfakes without user agreement and demand verification that the content was produced using artificial intelligence (Quirk, 2023).

Challenges Ahead

3.1. Punishing the Perpetrator

Punishing the perpetrators of deepfake misuse presents a significant challenge, but this does not mean that such a challenge cannot be overcome. One limitation of existing laws is their strong relation with national jurisdictions, which proves problematic given the borderless nature of deepfake technology and difficulty in navigating transnational laws. Enhancing international cooperation and coordination to streamline the prosecution of cross-border deepfake cases may help to overcome such a limitation. Thus, the Bletchley Declaration, which was adopted by the nations who participated in the AI Safety Summit in November 2023, was a crucial international move that reaffirmed the necessity of continuing to use AI safely (Department for Science, Innovation & Technology, Foreign, Commonwealth & Development Office et al., 2023).

The anonymity of many malicious actors makes them difficult to trace, further complicating legal proceedings. To overcome this difficulty, regulations that facilitate the sharing of IP by social media companies, where deepfakes are most prevalent, and finding an interlocutor for such requests are useful. For example, Turkey's Social Media Law requires foreign social network companies with more than 1 million daily access to designate at least one person as a representative in Turkey (Bozkurt, 2021). This way, legal authorities can more easily direct IP-sharing requests. Increasing the technical and institutional capacity of the justice system to facilitate the tracking of individuals' digital signatures will also help to overcome this challenge. This is because many legal systems, including judges, prosecutors, and lawyers, find it difficult to understand technological crimes.

Malicious actors become especially difficult to track and punish if they are part of state-sponsored actors. The latter use more technically advanced technology and, therefore, are more difficult to track. However, once detected and attributed to a state, international law can be used to punish the perpetrator. At this point, states can also resort to international rules on state responsibility and request cessation of acts and reparation. Nonetheless, the threshold for attributing such wrongful acts to a state is particularly high.

As for copyright protections, especially related to celebrities, there is also a challenge arising from the fact that celebrities are often not the copyright owners of the images or videos used in deepfakes. This means the copyright owner, i.e. the person who "authored" a work other than the celebrity, such as a paparazzi, has the legal standing to pursue a copyright infringement claim. To address this issue, social media companies should take more responsibility for the self-removal of copyright-infringing content.

3.2. Platform Responsibility

Social media platforms greatly contribute to the spread of deepfakes. However, the rules about their responsibility for what's posted on their sites vary, and often, these platforms are not held responsible for the content shared on them. For instance, Section 230 of the Communications Decency Act in the United States absolves social media platforms of liability for content posted by users. This legal provision promotes freedom of expression on the one hand and paves the way for disinformation and the spread of deepfakes on the other.

Chief Executive Officer (CEO) of Meta, Mark Zuckerberg testify before a Senate Judiciary Committee hearing on online child sexual exploitation in the Dirksen Senate Office Building on January 31, 2024, in Washington DC, United States. (Celal Güneş - Anadolu Agency)

Recently, to address the downsides of social media companies' nonliability, lawmakers have been more inclined towards imposing more responsibility on social media companies. For instance, the Digital Services Act 2023 in the European Union requires big businesses to carry out risk analyses on the services they offer that make it possible for unlawful content to be distributed, as well as to put in place and execute effective mitigation strategies. Similarly, the Online Safety Act of the UK, to that end, imposes a duty to identify, manage, and mitigate the risk of harm to providers, including social media platforms. The act also provides for imposing fines of up to £18m or 10% of global turnover (Online Safety Act, 2023).

Corporate social responsibility may be another option to ensure that platforms bear responsibility. The corporate social responsibility framework of human rights law sets forth voluntary obligations for companies, requiring companies to act with due diligence to avoid infringing others' rights as well as to take measures adequate for preventing, mitigating, and remedying human rights violations. The problem with this framework, however, is that these obligations are non-binding and do not provide enough incentives for companies to take measures that would reduce their profitability.

3.3. Freedom of Expression

The biggest concern raised by the regulations on deepfakes is the risk of disproportionate interference with fundamental rights and freedoms, especially freedom of expression. Thus, regulations must strike a delicate balance between combatting the harms associated with deepfakes and respecting human rights. Accordingly, banning all deepfakes would violate human rights and be against the constitutions of most countries. On the other hand, banning those that involve libel, defamation, and obscenity may be justified and legitimate. Alternatively, incorporating markers on deepfake content to indicate manipulation and requiring a text statement acknowledging the modification, as proposed in the yet-to-be-enacted DEEPFAKES Accountability Act of the US, offers a more nuanced approach. This approach not only aims to deter malicious manipulation but also empowers victims to seek legal recourse for damage to their reputation, thereby promoting accountability and responsible use of deepfake technology.

Additionally, when social media companies rely on their contractual powers in terms and conditions for content moderation, it should be proportionate in terms of human rights intervention against the misuse of deepfakes.

In social media companies' content moderation, there are generally lower free speech standards, a lack of transparency and accountability, and insufficient procedural safeguards and remedies regarding human rights (Article 19, 2023). To protect human rights in this regard, both social media companies should establish better standards, and governments should set standards for social media companies' content moderation.

3.4. Keeping Up with the Pace of Deepfake Technology

Deepfake technology is progressing rapidly, becoming more advanced with each development. This makes it increasingly difficult to address the problem of malicious deepfakes. For instance, in 2018, University of Albany researchers identified irregularities in blinking as a key indicator of fake videos, which would help to detect malicious deepfake content with the eye (Galston, 2020). However, this breakthrough soon lost its effectiveness as new deepfake videos quickly addressed this flaw.

One solution to address the rapid evolution of deepfake technology is to establish ongoing research and development initiatives focused on detecting and mitigating deepfake manipulation. By investing in cutting-edge technologies and interdisciplinary collaborations, researchers can stay ahead of emerging threats and continuously improve detection methods. Additionally, fostering partnerships between academia, industry, and government agencies can facilitate the sharing of expertise and resources to develop more robust countermeasures against deepfake misuse.

Education and awareness campaigns are also crucial in addressing the challenges posed by deepfakes. By educating the public about the risks associated with deepfake technology and providing guidance on how to identify and report suspected deepfakes, individuals can become more knowledgeable consumers of digital content. Empowering users with the knowledge and tools to evaluate media sources critically can help mitigate the spread of misinformation and reduce the impact of deepfake manipulation on society.

3.5. Innovation v. Regulation: Struggle of Low- and Middle-Income Countries

Regulating deepfakes requires thoughtful planning to avoid stifling innovation, particularly in low and middle-income countries where the AI industry is still emerging. Solutions to this challenge are like those applied in other sectors, including implementing a risk-based approach to technology policy, collaborating with industry stakeholders, and enhancing institutional and legal capacity for AI, especially in less advanced nations in the AI industry. Additionally, fostering international cooperation and knowledge-sharing initiatives can help these countries navigate regulatory challenges and accelerate their progress in adopting effective deepfake regulation.

Conclusion

As deepfake technology continues to evolve and proliferate, urgent action is needed to address the risks it poses to individuals, societies, and democratic processes. The widespread dissemination of deepfakes threatens privacy, undermines trust in information, and enables malicious activities with far-reaching consequences.

Therefore, a multifaceted approach is necessary, involving the enhancement of legal frameworks, the promotion of international cooperation, and the advancement of technological solutions. Governments must enact comprehensive legislation targeting deepfake misuse, while social media platforms must assume greater responsibility for content moderation. Moreover, efforts to keep pace with evolving deepfake technology through ongoing research and development initiatives are crucial.

Finally, it is imperative to strike a balance between innovation and regulation, ensuring that regulatory measures do not stifle technological advancements, particularly in low and middle-income countries. By taking concerted action, we can mitigate the risks posed by deepfakes and safeguard the integrity of our digital landscape for future generations.

References

Ambrose, T. (2024, February 25). UK's enemies could use AI deepfakes to try to rig election, says James Cleverly. *The Guardian*. https://www.theguardian.com/uk-news/2024/feb/25/uks-enemies-could-use-ai-deepfakes-to-try-to-rig-election-says-james-cleverly

An act to add Section 1708.86 to the Civil Code, relating to privacy, Cal. Assemb. B. 602, Chapter 491 (Cal. Stat. 2019). https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201920200AB602

Aouf, R. S. (2019, May 24). Museum creates deepfake Salvador Dali to greet visitors. *Dezeen*. https://www.dezeen.com/2019/05/24/salvador-dali-deepfake-dali-museum-florida/

Article 19. (2023, August). *Content moderation and freedom of expression handbook*. https://www.article19.org/wp-content/uploads/2023/08/SM4P-Content-moderation-handbook-9-Aug-final.pdf

Artz, K. (2019, October 11). Texas outlaws 'Deepfakes'—but the legal system may not be able to stop them. https://www.law.com/texaslawyer/2019/10/11/texas-outlaws-deepfakes-but-the-legal-system-may-not-be-able-to-stop-them/#:~:text=Texas%20Senate%20Bill%20751%20(SB751,and%20offenders%20can%20be%20sentenced

Bass, D. F., & Penning, N. (2023, July 25). The legal issues surrounding deepfakes. *Honigman*. https://www.honigman.com/the-matrix/the-legal-issues-surrounding-deepfakes

Bozkurt, N. D. (2021, May 7). Sosyal ağ sağlayıcılarının Türkiye'de temsilci atama yükümlülüklerinde son durum. *Moral Kınıkoğlu Pamukkale*. https://moral.av.tr/tr/makaleler/sosyal-ag-saglayicilarinin-turkiyede-temsilci-atama-yukumluluklerinde-son-durum-484#:~:text=Kural%20nedir%3F,temsilci%20olarak%20belirleme%20zorunluluğu%20getirilmiştir

Canadian Criminal Code, R.S.C. c. C-46 (1985). https://laws-lois.justice.gc.ca/eng/acts/c-46/section-163.1.html

Catenacci, C. (2024, February 23). The problem with deepfakes, and British Columbia's solution. *First Reference*. https://blog.firstreference.com/the-problem-with-deepfakes-and-british-columbias-solution/

Department for Science, Innovation & Technology, Foreign, Commonwealth & Development Office, & Prime Minister's Office. (2023, November 1). *The Bletchley Declaration by countries attending the AI Safety Summit, 1-2 November 2023* [Policy paper]. https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023

Durbin, R. J., & Graham, L. (2024). The DEFIANCE Act of 2024. https://www.durbin.senate.gov/imo/media/doc/defiance_act_of_2024.pdf

Edelman, A. (2024, January 23). States turn their attention to regulating AI and deepfakes as 2024 kicks off. *NBC News*. https://www.nbcnews.com/politics/states-turn-attention-regulating-ai-deepfakes-2024-rcna135122

European Parliament & Council of the European Union. (2016, May 4). *Regulation (EU) 2016/679 of the European Parliament and of the Council*. https://iapp.org/resources/article/the-eu-general-data-protection-regulation/#A17

Galindo, G. (2020, April 14). XR Belgium posts deepfake of Belgian premier linking Covid-19 with climate crisis. *The Brussels Times*. https://www.brusselstimes.com/106320/xr-belgium-posts-deepfake-of-belgian-premier-linking-covid-19-with-climate-crisis

Galston, W. A. (2020, January 8). *Is seeing still believing? The deepfake challenge to truth in politics*. The Brookings. https://www.brookings.edu/articles/is-seeing-still-believing-the-deepfake-challenge-to-truth-in-politics/

Geller, E., & Vinocur, N. (2017, May 5). French presidential candidate confirms 'massive' hack days before election. *Politico*. https://www.politico.com/story/2017/05/05/emmanuel-macron-french-election-hack-cyber-238059

Narcisse, E. (2017, December 8). It took some movie magic to complete Carrie Fisher's Leia dialogue in The Last Jedi. *Gizmodo*. https://io9.gizmodo.com/it-took-some-movie-magic-tocomplete-carrie-fishers-lei-1821121635

Nealy, D. (2023, February 2). This Seinfeld/Pulp Fiction deepfake is a little too good. *Boingboing*. https://boingboing.net/2023/02/02/this-seinfeld-pulp-fiction-deepfake-is-a-little-too-good.html

NO FAKES Act of 2023, EHF23968 GFW, (2023). https://www.coons.senate.gov/imo/media/doc/no_fakes_act_draft_text.pdf

Online Safety Act 2023, c. 50, https://www.legislation.gov.uk/ukpga/2023/50/enacted

Quirk, C. (2023, June 19). The high stakes of deepfakes: The growing necessity of federal legislation to regulate this rapidly evolving technology. *Princeton Legal Journal*. https://legaljournal.princeton.edu/the-high-stakes-of-deepfakes-the-growing-necessity-of-federal-legislation-to-regulate-this-rapidly-evolving-technology/

Sarnoff, L. (2024, January 30). Taylor Swift and No AI Fraud Act: How Congress plans to fight back against AI deepfakes. *abcnews*. https://abcnews.go.com/US/taylor-swift-ai-fraud-act-congress-plans-fight/story?id=106765709

Secretary of the World Intellectual Property Organization. (2020, May 21). *WIPO Conservation on intellectual property (IP) and artificial intelligence (AI)*. https://www.wipo.int/edocs/mdocs/mdocs/en/wipo_ip_ai_2_ge_20/wipo_ip_ai_2_ge_20_1_rev.pdf

Shakeri, A. (2018, April 14). Lyrebird Helps ALS Ice Bucket Challenge Co-Founder Pat Quinn Get His Voice Back: Project Revoice Can Change Lives. *Huffington Post*. https://www.huffingtonpost.ca/2018/04/14/lyrebird-helps-als-ice-bucket-challenge-co-founder-patquinn-get-his-voice-back_a_23411403

Talas, T., & Kearney, M. (2019, September). Diving into the deep end: Regulating deepfakes online. *Communications Law Bulletin Vol 38.3*. https://www5.austlii.edu.au/au/journals/CommsLawB/2019/24.pdf

The White House, (2023, October 30). *President Biden Issues Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence* [Fact sheet]. https://www.whitehouse.gov/briefing-room/statements-releases/2023/10/30/fact-sheet-president-biden-issues-executive-order-on-safe-secure-and-trustworthy-artificial-intelligence/

Turkish Criminal Code, 5237 (2004). https://www.mevzuat.gov.tr/mevzuat?MevzuatNo=5237&MevzuatTur=1&MevzuatTertip=5

U.S. Senate Committee on the Judiciary. (2024, January 30). *Durbin, Graham, Klobuchar, Hawley introduce DEFIANCE Act to hold accountable those responsible for the proliferation of nonconsensual, sexually-Explicit "Deepfake" images and videos*. https://www.judiciary.senate.gov/press/releases/durbin-graham-klobuchar-hawley-introduce-defiance-act-to-hold-accountable-those-responsible-for-the-proliferation-of-nonconsensual-sexually-explicit-deepfake-images-and-videos

Vincent, J. (2018, April 17). Watch Jordan Peele use AI to make Barack Obama deliver a PSA about fake news. *The Verge*. https://www.theverge.com/tldr/2018/4/17/17247334/ai-fake-news-video-barack-obama-jordan-peele-buzzfeed

Weatherbad, J. (2024, January 25). Trolls have flooded X with graphic Taylor Swift AI fakes. *The Verge*. https://www.theverge.com/2024/1/25/24050334/x-twitter-taylor-swift-ai-fake-images-trending

TRT WORLD
research centre

TRTWORLD
research
centre