

# 2025-1

SLTA TECH & LAW INSIGHTS

# FAKE IT 'TIL YOU MAKE IT...ILLEGAL

THE PATCHWORK OF GLOBAL DEEPPFAKE LAWS

BRECHTJE LINDEBOOM, CRYSTAL DUBOIS

---

Editorial Team :

Nicolas Torrent, Nomungerel Jamsranjav, Ziyu Liu



## INTRODUCTION

---

As generative AI technology becomes more accessible, so do deepfakes. Deepfakes use artificial intelligence to create highly realistic and convincing fake images, videos, and audio.<sup>1</sup> It blurs the lines between reality and fiction, posing serious threats across various sectors.

The dangers of deepfakes range from spreading political disinformation<sup>2</sup> and undermining trust in public figures to enabling sophisticated financial fraud and cybercrime.<sup>3</sup> They also present a major challenge to intellectual property rights and personal identity, as seen in the music industry's fight against unauthorized AI-generated content.<sup>4</sup> Ultimately, deepfakes threaten to compromise the integrity of media, the security of our finances, and the authenticity of human expression.

According to Resemble.ai, a company specializing in deepfake detection, in the second quarter of 2025, there were 487 reported attacks, marking a 41% increase from the previous quarter and a more than 300% rise year-over-year.<sup>5</sup>





## LEGISLATIVE INITIATIVES

---

Legislators have been taking action. The U.S. has adopted the ‘TAKE IT DOWN Act’, with another bill, the ‘NO FAKES Act’, currently making its way through Congress.<sup>6</sup> Meanwhile, the EU’s AI Act mandates that users of AI technology disclose it when content has been artificially created or manipulated.<sup>7</sup>

Recently, Denmark has announced an amendment to the existing Copyright Act that grants individuals legal ownership of their own physical likeness, including their face, body, and voice, to protect them from unwanted deepfakes.<sup>8</sup> In the Netherlands, Dutch parliamentarians are considering amending the country’s Neighbouring Rights Act to address deepfakes,<sup>9</sup> despite a 2022 study concluding that Dutch law already provides sufficient protections against deepfakes.<sup>10</sup>

In Switzerland, no special law exists against deepfakes. In November 2023 it was confirmed that the Swiss Data Protection Act (DPA) applies directly to AI<sup>11</sup>. In May 2025, the Federal Data Protection and Information Commissioner confirmed that deepfake content, which fabricates or alters the faces, images, or voices of identifiable individuals, must be clearly labelled to ensure transparency.<sup>12</sup>

The DPA also requires that AI systems be transparent about their purpose and data sources, giving individuals the right to object to automated data processing. Switzerland’s legal framework against deepfakes includes the Swiss Civil Code (art. 28 for personality rights including image rights), Swiss Criminal Code (for defamation, identity theft and ‘revenge porn’), the Data Protection Act (privacy violations) and the Federal Act on Copyright and Related Rights (for infringement of authors’ and performers’ rights).<sup>13</sup>

The question arises, therefore, whether new legislation is indeed needed to address deepfakes, and if so, whether copyright and neighbouring rights are best suited to do so. Bernt Hugentholtz, Professor at the Institute for Information Law, underlines that copyright and intellectual property laws exist to create a market for creative works, not to prevent their use.<sup>14</sup> Their primary goal is to encourage the spread of content by providing a framework that compensates creators.



Whilst he acknowledges that there may be good reasons to create stronger protection for performing artists, he argues: *“Is granting every person a new IP right the best way to deal with deepfakes? I don’t think so. Although to a hammer everything may look like a nail, IP law is only one of many instruments in the lawmaker’s toolkit. If concerns over privacy and reputation are the main reasons for regulating deepfakes, any new rules should be grounded in the law of privacy. If preserving trust in the media or safeguarding democracy are the dominant concerns, deepfakes ought to be addressed in media regulation or election laws.”*<sup>15</sup>

## CONCLUSION

---

While stronger protections for performing artists may be needed, existing laws already provide a wide range of legal options against deepfakes. There is nothing wrong with Denmark embedding additional wording in support of creators into its existing Copyright Act. At the same time, granting every citizen a copyright on their face, voice and physical expression in order to protect them against deepfakes may be a bridge too far.

The purpose of copyright is to compensate creators, not to shield citizens from fake porn, fraudulent videos, or defamatory content. The unauthorized use of an individual’s likeness and/or voice in deepfake porn or to commit fraud can be addressed through both civil law (specifically, tort) and criminal law.

Legislators must be careful to balance the need to address deepfakes by changing existing laws on the one hand, with the risk of overregulation and creating an unclear legislative patchwork on the other hand. For some countries, a hybrid framework, whereby existing laws are updated and a new law is introduced, may offer the best result.

As legislators advance, the impact eventually will hinge on precise legal definitions, platform compliance, and, last but not least, coordinating enforcement across borders. As researchers have pointed out, actually enforcing rights and remedies against anonymous perpetrators in unknown locations remains nearly impossible – a recurring internet challenge.<sup>16</sup>



## REFERENCES

---

1. [What is Deepfake Technology? | Definition from TechTarget](#)
2. [Fake Biden New Hampshire robocall most likely AI-generated](#)
3. [How Ferrari Hit the Brakes on a Deepfake CEO](#)
4. [Katy Perry, Billie Eilish, J Balvin and more lash out against ‘enormous’ AI threats that ‘sabotage creativity’ | CNN Business](#) [Celine Dion warns fans to beware of fake, AI-generated songs appearing online | CNN](#)
5. “Q1 2025 Deepfake Incident Report: Mapping Deepfake Incidents”, [Q1 Deepfake Threats](#)
6. [Deepfake Regulation Overview: All About AI and Deepfake Laws](#)
7. [Article 50: Transparency Obligations for Providers and Deployers of Certain AI Systems | EU Artificial Intelligence Act](#)
8. [Denmark’s Groundbreaking Move: Copyright for Faces and Voices - GLOBAL LAW TODAY](#)
9. [The Dutch and Danish proposals for legislation on deepfakes](#)
10. [NL] Report for Government on the regulation of deepfake technology, Arlette Meiring Institute for Information Law (IViR), University of Amsterdam, IRIS 2022 [Article](#)
11. Current data protection legislation is directly applicable to AI, the Swiss Federal Data Protection and Information Commissioner (FDPIC), published on 9 November 2023 ([Communication](#))
12. Update - Current data protection legislation is directly applicable to AI, the Swiss Federal Data Protection and Information Commissioner (FDPIC), published on 8 May 2025  
[Update - Current data protection legislation is directly applicable to AI](#)
13. Defamation and Privacy Law in Switzerland, Corinne Corminboeuf Harari  
[Switzerland - Carter-Ruck](#)    [The protective parameters of civil and constitutional personality rights in Swiss law](#)
14. Deepfake Bills in Denmark and the Netherlands: Right idea, wrong legal framework. [P. Bernt Hugenholtz](#) (Institute for Information Law (IViR)) August 6, 2025
15. Deepfake Bills in Denmark and the Netherlands: Right idea, wrong legal framework. [P. Bernt Hugenholtz](#) (Institute for Information Law (IViR)) August 6, 2025
16. [NL] Report for Government on the regulation of deepfake technology, Arlette Meiring Institute for Information Law (IViR), University of Amsterdam, IRIS 2022 [Article](#)  
[Deepfake Bills in Denmark and the Netherlands: Right idea, wrong legal framework. | Kluwer Copyright Blog](#)