Deepfakes and Digital Identity: What Pakistan Can Learn from Denmark's Deepfake Law

Author: Maham Nasir

Keywords: Deepfakes; Digital Laws; Pakistan Cyber Laws; National AI Policy 2025; Denmark Copyright Act; PECA; AI Impersonation, Digital Identity; Post-Mortem Rights.

Introduction:

In present times, when Artificial Intelligence ('AI') use is rampant across all spheres of life, a stricter technological regulation needs to be introduced in the domestic legal system to ward against the emerging cyber threats. The 'deepfake' technology has progressed simultaneously with the rise of AI and has now become a challenge for Pakistan's cybercrime framework. Different jurisdictions have enacted laws to tackle the issue. One way is that the person's voice, body parts, and more broadly, 'likeness' is declared to be their property. Such a regime clearly provides a statutory right to demand the takedown of any content using a person's property without their consent, thereby circumventing lengthy judicial proceedings by providing pre-emptive remedies to the victim.[1] This is the model of the recently proposed amendment to the Danish Copyright Act ('Amendment').[2] Other jurisdictions, like Pakistan, are still operating under a set of outdated laws, which have been inadequate to address the novel challenges posed by AI-generated deepfakes.[3] This article examines the 2025 Amendment to the Danish Copyright Act to draw inspiration for Pakistan's cyberspace legal framework.

---

[1] Henry Patishman, 'Deepfake Regulations: AI and Deepfake Laws of 2025' (Regula Forensics, 12 August 2025) <https://regulaforensics.com/blog/deepfake-regulations/> accessed 24 December 2025.

[2] Danish Copyright (Amendment) Act 2025.

[3] Fatima Rida Suddle, Aden Khan and Sehar Nawaz, 'The Legislative Framework for Cybercrime in Pakistan: A Critical Analysis of PECA 2016' (2025) 3(8) Annual Methodological Archive Research Review 1 <https://amresearchjournal.com/index.php/Journal/article/view/467> accessed 24 December 2025.

The Deepfake Phenomenon: A Global Crisis

Deepfakes are AI-generated images, audio, or videos that hyper-realistically resemble any dead or living human and falsely appear to be authentic or truthful.[4] United Nations Educational, Scientific and Cultural Organization ('UNESCO') recently labelled synthetic content a 'crisis', noting that the generative AI market is expected to grow by 560% between 2025 and 2031, reaching an estimated value of $442 billion.[5] Deepfakes have become so common that even prominent global figures like Taylor Swift[6] and the Princess of the Dutch royal family[7] are struggling to fight them. Pakistan, too, has had its fair share of controversies, from staged drone strikes at cricket stadiums[8] to videos of the chief minister allegedly revealing sensitive policies during state meetings.[9] Yet the local laws remain insufficient to tackle deepfakes effectively.

Deepfake Challenges and Vulnerabilities in Pakistan

Before examining the Danish model, it is crucial to first understand the challenges and vulnerabilities that Pakistan faces in relation to AI-generated content.

---

[4] Council Regulation (EC) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L168/1 <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng> accessed 24 December 2025.

[5] Dr Nadia Naffi, 'Deepfakes and the Crisis of Knowing' (UNESCO, 1 October 2025, last updated 27 October 2025) <https://www.unesco.org/en/articles/deepfakes-and-crisis-knowing> accessed 24 December 2025.

[6] Halle Nelson, 'Taylor Swift and the Dangers of Deepfake Pornography' (National Sexual Violence Resource Center, 7 February 2024) <https://www.nsvrc.org/blog_post/taylor-swift-and-dangers-deepfake-pornography/> accessed 24 December 2025.

[7] James Moules, 'Royal Princess Targeted by Deepfake as Cops Investigate Netherlands Case' (The Sun, 18 August 2025) <https://www.thesun.co.uk/news/36339189/royal-princess-deepfake-cops-netherlands> accessed 24 December 2025.

[8] Zainab Bawa and Navkiran S. Dhillon, 'In South Asia, Deepfakes Are Increasingly Used to Inflict Gendered Harm' (Digital Rights Monitor Pakistan, 12 November 2024). <https://digitalrightsmonitor.pk/in-south-asia-deepfakes-are-increasingly-used-to-inflict-gendered-harm/> accessed 24 December 2025.

[9] Staff Reporter, 'Deepfakes weaponized to target Pakistan's women leaders' *Arab News Pakistan* (Lahore, 3 December 2024) <https://www.arabnews.pk/node/2581581/pakistan> accessed 24 December 2025.

I. Legal Gaps in Current Cyber Laws

As technology evolves, Pakistan faces the challenge of aligning its legal framework with technological advancements. The recent amendment to the Prevention of Electronic Crimes Act[10] ('PECA amendment') criminalises the 'intentional dissemination, public exhibition, or transmission of any information through any system that a person knows, or has reason to believe, is false or fake'. It also adds the term aspersion and defines it as disseminating information which is false and damages reputation.[11] While these provisions formally cover false information and reputational harm, they focus only on the intent of the content being disseminated and not the technology used to generate it, which is inadequate because deepfakes arise from technological manipulation of reality regardless of the intent, thus making intent-based threshold structurally insufficient.[12] Furthermore, the cases filed following the PECA amendment mostly concern misleading information and hate content rather than synthetic media,[13] highlighting that the law works more like a speech-regulating tool, rather than a statute addressing deepfake-specific harms.[14]

The National AI Policy 2025 is another attempt to stabilise the relationship between the state and AI platforms. Although the policy aims to create a robust AI environment and addresses major problems like digital literacy, it still leaves unaddressed technological manipulation, clear evidentiary standards for digital offences, and precise provisions defining deepfakes.[15]

---

[10] The Prevention of Electronic Crimes (Amendment) Act 2025, s 26 A.
[11] Ibid s2R(h).
[12] Robert Chesney and Danielle K Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 *California Law Review* 1753, 1763–1768.
[13] Staff Reporter, 'Punjab police file three cases under PECA for deepfake content' *Dawn* (21 February 2025); 'Lahore Police registers over 23 cases for PECA violation in 24 hours' *Aaj English TV* (24 April 2025); 'Over 350 Pakistanis booked under illegal cases under PECA Act' *Daily Pakistan* (10 September 2025).
[14] Human Rights Commission of Pakistan (n 9).
[15] Staff Reporter, 'Cabinet Approves National AI Policy 2025 to Build Robust AI Ecosystem' (Aaj English TV, 31 July 2025)<https://english.aaj.tv/news/330427165/cabinet-approves-national-ai-policy-2025-to-build-robust-ai-ecosystem> accessed 24 December 2025.

II. Digital Rights After Death

Pakistan also fails to recognise digital rights after death.[16] When a person dies, data stored on cloud services or digital platforms is often left unregulated, creating the risk of unauthorised access and misuse by AI technologies to generate fabricated content. While several jurisdictions have begun to recognise post-mortem digital rights,[17] Pakistan continues to lag due to its limited recognition of digital identity and the absence of rules governing digital accounts after death.

III. Societal and Infrastructural Vulnerabilities

Beyond legislative lacunae, Pakistan also experiences the widespread irresponsible use of digital spaces, making them hard to regulate. Currently, Pakistan's digital footprint includes approximately 117 million users.[18] With such widespread access to the internet and social media platforms, particularly TikTok, which has an audience of 66.9 million users aged 18 and above,[19] the circulation of unverified synthetic content is amplified. TikTok mainly targets users aged 13 and above, many of whom are adolescents with limited ability to verify information.[20] As a result, the app has become one of the most efficient channels of disseminating digital forgeries. While platforms like Facebook and YouTube use AI-based detection mechanisms, these systems are primarily trained on English-language content, allowing material in Urdu and other regional languages to evade scrutiny.[21]
Moreover, these platforms often escape accountability due to their extra-territorial nature, thus

[16] Alisha Tahir and Ishtiaq Ahmed, 'Why Pakistan Urgently Needs Digital Will Legislation in the AI Era: Insights from the United Kingdom' [2025] SSRN 1-3 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5844482> accessed 08 Feb 2026.
[17] Edina Harbinja, Tal Morse and Lilian Edwards, 'Digital remains and post-mortem privacy in the UK: what do users want?' [2025] International Review of Law, Computers & Technology 1 <https://doi.org/10.1080/13600869.2025.2506164> accessed 24 December 2025.
[18]Simon Kemp, 'Digital 2026: Pakistan' (DataReportal, 2026) <https://datareportal.com/reports/digital-2026-pakistan> accessed 24 December 2025.
[19] Ibid.
[20] Nosharwan Arbab Abbasi and Dianlin Huang, 'Digital Media Literacy: Social Media Use for News Consumption among Teenagers in Pakistan' (2020) 18(35) *Global Media Journal* 1.
[21] Fatima Rida Suddle (n 3).

falling outside the jurisdiction of local courts, which creates a gap that amplifies deepfake proliferation.

IV. Victim Blaming and Slow Processes

Victim blaming has long been at the core of cybercrime in Pakistan. One of the most common uses of deepfakes is the creation of so-called 'revenge porn', which disproportionately targets women.[22] Due to prevailing societal attitudes that stigmatise victims instead of perpetrators, nearly 68% of Pakistani women facing deepfake-related harassment are forced to answer questions like why they were online in the first place or why they posted their photographs at all.[23]

This mindset highlights the fact that in societies where honour means more than the life of the victims, asserting one's legal rights becomes extremely difficult. Even when victims muster courage and take up the odious task of reporting deepfake content, the process is so painfully slow that the harmful content stays on the internet for too long after the damage has already occurred. This highlights the urgent need to have effective safeguards against digital rights violations.

The Danish Model

The recent Amendment to the Danish Copyright Act is one of the most groundbreaking AI- related legislative initiatives of 2025.[24] Proposed in June 2025 and expected to be implemented by late 2025 or early 2026, this new legislation inserts Sections 65a and 75a into the existing Danish Copyright Act. With its remarkable features, the Amendment creates a comprehensive legal framework to counter the harms posed by deepfakes.

---

[22] Syeda Samana Ameer, 'Deepfakes: A Crisis of Human Rights' (Research Society of International Law Pakistan, 19 April 2024) <https://rsilpak.org/2024/deepfakes-a-crisis-of-human-rights/> accessed 24 December 2025.

[23] Syed Messum Ali Kazmi, Rabia Iftikhar and Muhammad Umar Fayyaz, '"It Is All Her Fault": Psychosocial Correlates of the Negative Attitudes towards Rape Victims among the General Population of Pakistan' (2023) 13 *Egyptian Journal of Forensic Sciences 2* <https://doi.org/10.1186/s41935-022-00320-3> accessed 24 December 2025.

[24] Henry Patishman, 'Global Legal Actions Against AI Deepfakes: Five Laws of 2025' (Regula Forensics, 12 August 2025) <https://regulaforensics.com/blog/deepfake-regulations/> accessed 24 December 2025.

Firstly, the Amendment explicitly defines deepfakes as the hyper-realistic digital representation of any human, including voice and physical appearance.[25] Following this definition, the Amendment introduces a right of one of its own kinds, known as the 'personality right', which functions like copyright or intellectual property rights. This right enables individuals to prevent unauthorised use of their likeness. Exercising this right, victims can immediately demand that any platform (local or international) take down the violative content, thus providing an effective remedy before any significant harm to their reputation.

The right has an expansive territorial scope, as it is not confined to Danish nationals, but extends to any natural person whose likeness is reproduced or disseminated within Denmark's territorial jurisdiction, a significant feature in today's transnational digital context.

Secondly, the Amendment recognises the digital rights not just for the period of a person's natural life but stipulates that the legal protection 'shall last 50 years after the death of the person imitated', representing an extraordinary step towards digital post-mortem rights.[26]

Lastly, the wording of the proposed legislation explicitly states that the granted right covers 'every type of deepfake', not merely those created for sexual exploitation, fraud, or blackmail. This includes content that may not be a replica but is functionally equivalent and capable of producing the same deceptive effect.[27]

Notably, the Amendment also seeks to strike a balance between digital rights and freedom of expression by exempting bona fide imitations. Consistent with the 'fair use doctrine', the Amendment applies only to 'realistic digitally generated imitations' of a person and exempts caricature, satire, parody, pastiche, and criticism of power and society, all of which remain

[25]Abou Naja IP, 'Denmark's Deepfake Legislation: Bold Copyright and Digital Identity Protection' (15 August 2025) <https://abounaja.com/blog/denmarks-deepfake-legislation-bold-copyright-and-digital-identity-protection> accessed 24 December 2025.
[26] Ibid.
[27] Colin Lambertus, 'Denmark Proposes to Protect Individuals from AI Deepfakes by Making Changes to Its Copyright Laws' (EM Law, 23 July 2025) <https://emlaw.co.uk/denmark-proposes-to-protect-individuals-from-ai-deepfakes-by-making-changes-to-its-copyright-laws/?utm_source=chatgpt.com> accessed 24 December 2025.

protected unless they constitute misinformation. Where such exceptions result in serious harm to the public due to misinformation, it may then become actionable.

Denmark vs. Pakistan: A Comparison and Some Recommendations

A plain reading of the Danish model reveals several features, including a clear definition of deepfake embedded in a personal rights framework, pre-emptive remedies, and postmortem digital identity; all of these features are absent in the Pakistani legal system.

Pakistan, in contrast, addresses deepfakes only after the damage is done. In the absence of a proper definition and recognition of the actual issues, victims still have to rely on fragmented criminal law remedies that focus on intent rather than harm. Therefore, digital identity, both during life and death, remains largely unrecognised in Pakistan, while platform responsibility is minimal as most digital platforms have no local presence, thus restricting the jurisdiction of domestic courts. In essence, the legislative intent in Denmark is victim-centric and focuses on swift, pre-emptive remedies, whereas Pakistan's legal framework remains reactive, slow, and ineffective.

In light of the analysis above, several policy and legal practices are recommended to mitigate the increasing threat of deepfakes in Pakistan. To name a few:

I. Stringent Laws:

Pakistan's legal system currently does not recognise synthetic manipulation as a distinct offence. Priority should be given to defining 'deepfakes' as a personality right violation and an offence against a person's dignity to be compensated with damages, in addition to imprisonment.

II. Strict Platform Compliance:

Pakistan should consider creating a national regulatory authority to specifically manage the deepfake violations against international platforms and ensure immediate execution of removal requests, as Denmark operates by appointing a digital service coordinator to implement the digital

laws.[28] Non-compliance by international platforms, including failure to establish local offices, should also result in strict penalties.

III. Training Programs:

Specialised training programs for judges, prosecutors, and law enforcement agencies should be introduced in the same way as Denmark trains its judicial personnel through programs initiated by the national cybercrime center[29] to improve the detection, enforcement and adjudication of deepfake-related offences. Gender-sensitive training should also be prioritised, given the disproportionate impact of deepfakes on women.

IV. Proactive Victim Centric Approaches:

Unlike Pakistan's current reactive system that comes into action after the damage is done, laws should intervene before harm materialises through pre-emptive takedown mechanisms and digital monitoring similar to the above-discussed Danish model. Anonymous support mechanisms must also be established to protect victims from societal pressure and stigmatisation.

Conclusion:

Deepfakes pose serious threats to human dignity. While countries like Denmark are adopting modern legislative responses, Pakistan continues to rely on outdated frameworks. However, due to various constitutional, institutional, and cultural differences, replicating the Danish model is not possible for Pakistan. Nonetheless, some features, such as the legal definition of deepfakes and recognition of personality rights beyond life, are directly transferable. Other components, such as platform compliance and training and awareness mechanisms, may be adopted according to the constitutional structure and enforcement capacity.

---

[28] European Union, 'Denmark—Policy Monitor Country Profile' (2025) <https://better-internet-for-kids.europa.eu/en/knowledge-hub/denmark-policy-monitor-country-profile> accessed 16 January 2026.

[29] Council of the European Union, 'The Practical Implementation and Operation of European Policies on Prevention and Combating Cybercrime - Report on Denmark' (June 2017) <https://www.parlament.gv.at/dokument/XXV/EU/146309/imfname_10726387.pdf> accessed 08 Feb 2026.

Any meaningful reform must first begin with acknowledging and protecting digital identity as a legal interest. Without such recognition, technological advancement will continue to outpace legal safeguards, with consequences extending beyond individual harm to public trust in law and governance.