

Francesca Portante D'Alessandro

FWO PhD Fellow at KU Leuven Centre for IT and IP Law (CiTiP)

Modern problems (do not) require modern solutions: A critical assessment of the Dutch and Danish copyright proposals for regulating deepfakes

Abstract: The online dissemination of deepfakes has intensified concerns about the protection of individuals against unauthorised digital representations that may harm individuals' fundamental rights, prompting extensive debate across the EU. In an effort to act against the reputational and psychological harms of deepfakes, recent Dutch and Danish bills have suggested granting individuals copyright and neighbouring rights over their likeness in digital representations. This paper critically examines whether copyright law is an appropriate tool to address the harms caused by non-consensual deepfakes, or whether existing legal frameworks already offer sufficient protection. The paper contends that amendments to national copyright law are ultimately ill-suited in providing effective protection and enforcement for victims, and policy efforts should rather be directed towards strengthening international cooperation and existing enforcement mechanisms to secure prompt and permanent removal of harmful content across jurisdictions.

1. INTRODUCTION

Long before the advent of Artificial Intelligence (AI), image and video manipulation have been a recurring phenomenon within the history of film and photography. Throughout the nineteenth century, photographers used hand-painting, multiple exposures, cropping and splicing to augment, manipulate or compose fictional scenes.¹ Early filmmakers likewise adopted in-camera tricks, matte paintings, and other analogue compositing techniques to create illusions.² Amongst famous "faked" images and videos are a portrait of Lincoln created by superimposing his head on a print of Calhoun's body³, or footage from the 1898 Spanish-American War splicing original footage from battles in Cuba and the Philippines with videos recreated in New Jersey.⁴

Advances in AI technology, particularly in generative modelling, have however radically revolutionised image and video manipulation, reducing the technical expertise, time and resources required.⁵ As a consequence, highly realistic fabricated (or "deepfaked") media can now be easily produced and rapidly disseminated by individuals with minimal technical training.⁶ Within this context, "deepfakes" have emerged as a distinctive category of AI-generated content circulating online. While no common standard definition exists amongst scholarship, deepfakes generally refer to synthetic images, audio, or videos created through deep learning techniques that convincingly replicate a person's likeness, voice, or features.⁷ It is important to note that the broader category of deepfakes is far from homogenous in nature.

¹ William J. Mitchell, *The Reconfigured Eye: Visual Truth in the Post-Photographic Era* (1994) pp.190-223

² Michael Z. Newman, *Video Revolutions: On the History of a Medium* (2024); Ken Dancyger, *The Technique of Film and Video Editing* (2010)

³ Fiona Macdonald, "How a 19th-Century portrait of Abraham Lincoln was later revealed to be a fake" BBC (14 March 2024) available at: <https://www.bbc.com/culture/article/20240313-how-a-19th-century-portrait-of-abraham-lincoln-was-later-revealed-to-be-a-fake>

⁴ US Library of Congress, "The Spanish-American War in Motion Pictures" available at:

<https://www.loc.gov/collections/spanish-american-war-in-motion-pictures/about-this-collection/>

⁵ Johannes Langguth et al, "Don't Trust Your Eyes: Image Manipulation in the Age of DeepFakes", *Front Commun* (2021)

⁶ *ibid*

⁷ Noemie Krack, "Exploring Legal Solutions for Non-Consensual Intimate and Sexually Explicit Deepfakes:

Meskys et al. identify 4 distinct sub-categories for classification: (i) commercial deepfakes, (ii) original deepfakes, (iii) political deepfakes and (iv) pornographic deepfakes.⁸ Commercial deepfakes help reduce transaction costs and facilitate the creation of new business models, as exemplified by translating video recordings into multiple languages.⁹ Original deepfakes include all deepfakes of a creative nature, such as parodies, “memes”, and entertainment content.¹⁰ Political deepfakes include politicians’ speeches and news reports, which may be used to promote political campaigns, damage national security or trust in government institutions.¹¹ Finally, pornographic deepfakes include both images and videos of individuals engaged in sexual acts, alongside intimate material such as nude images.¹²

While the democratisation of deepfake technologies offers vast applications in creative and commercial fields, where they can streamline post-production/visual effects and reduce transaction costs, it simultaneously amplifies potential risks of harms to individuals. This occurs in particular where deepfake technologies are used to generate or manipulate audio, video or images depicting real identifiable individuals without their knowledge or consent. Victims of such non-consensual deepfakes have been found to experience a wide range of interrelated psychological, social and economic harms, including reputational damage, anxiety and depression.¹³ Beyond individual impacts, deepfakes can also contribute to misinformation and gender-based violence online.¹⁴ The latter is well exemplified by the fact that over 95% of all deepfakes circulating online are of a pornographic nature, with close to 100% of victims being female.¹⁵

Deepfakes therefore raise significant concerns for individuals’ fundamental rights, most significantly the right to privacy¹⁶, personal integrity¹⁷ and human dignity¹⁸. Due to their very nature, pornographic and political deepfakes present heightened risks in this regard.¹⁹ Existing legal frameworks, such as fundamental rights, data protection, criminal law, and personality rights provide avenues for addressing the risks and harms of deepfake media to individuals. These general frameworks have additionally been complemented by new regulatory instruments at EU level explicitly addressing deepfakes, namely the Artificial Intelligence Act (AIA)²⁰, Digital Services Act (DSA)²¹ and Gender-Based Violence Directive

Insights from the AI Act, Gender-Based Violence Directive, and Digital Services Act”, *Auteurs en Media* 3/2024 (2025) p.337

⁸ Edvinas Meskys, “Aidas Liaudanskas, Julija Kalpokiene, Paulius Jurcys, Regulating deep fakes: legal and ethical considerations”, *Journal of Intellectual Property Law & Practice*, Volume 15, Issue 1 (2020)

⁹ *ibid*

¹⁰ *ibid*

¹¹ *ibid*

¹² *ibid*

¹³ Alexander Diel, “The harm of deepfakes: a scoping review of deepfakes’ negative effects on human mind and behavior”. *AI & Soc* (2025); Mariëtte van Huijstee, and others, *Tackling Deepfakes in European Policy* (European Parliament 2021); Krack (n7)

¹⁴ *ibid*

¹⁵ Ajder H. et al, *The State of Deepfakes: Landscape, Threats, and Impact* (2019); The Home Security Heroes, *2023 State Of Deepfakes: Realities, Threats, And Impact* (2024)

¹⁶ Art 7-8 Charter of Fundamental Rights of the European Union (CFR); Art 12 Universal Declaration of Human Rights (UDHR)

¹⁷ Art 3 CFR; Art 3 UDHR

¹⁸ Art 1 CFR; Art 1 UDHR

¹⁹ Krack (n7)

²⁰ Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)

²¹ Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)

(GBVD)²². Beyond these EU-wide measures, Member States are pursuing national strategies to tackle deepfakes. In 2021 Croatia amended its penal code to criminalise the creation and distribution of non-consensual sexually-explicit deepfakes, becoming the first EU country to introduce specific legal provisions to combat such phenomenon.²³ Similarly in 2024, the German Federal Council passed a draft law extending criminal law protection for personal rights against deepfakes.²⁴ Most notably, Denmark and the Netherlands have recently advanced legislative proposals that employ copyright and related rights to grant individuals stronger control over the unauthorised digital reproduction of their likeness to combat non-consensual deepfakes.²⁵ Such novel approach is aimed at strengthening existing regulatory approaches, enabling redress for victims. Critics have however questioned their efficacy, noting it remains unclear whether they provide effective protection beyond existing legal frameworks.²⁶ This issue currently remains largely unaddressed by copyright literature. The present paper examines the Dutch and Danish proposals, assessing the potential of copyright law as a regulatory tool for combating non-consensual deepfakes. The exploration is particularly relevant, as Denmark's 2026 presidency of the Council of the European Union may provide an opportunity to discuss the bill's potential broader implementation at EU.²⁷ To adequately evaluate the need for the proposed copyright law amendments, the present paper will first provide a brief overview of the ways in which copyright law is currently implicated in the creation and dissemination of deepfakes. It will then map how deepfakes are currently regulated at European and national Member State level. Finally, the Danish and Dutch bills will be analysed, highlighting potential benefits and limitations, with the aim of assessing to what extent copyright law may help tackle deepfakes and their associated harms.

2. COPYRIGHT IMPLICATIONS OF DEEPFAKES

Before assessing the potential of copyright to protect individuals from harmful deepfakes, it is essential to first understand how copyright law currently applies to the process of deepfake creation and distribution. As with generative AI more broadly, copyright law may be implicated at both input and output stages of the creation process. These issues have been extensively examined by copyright scholarship²⁸ and will therefore only briefly be presented herein.

²² Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence

²³ Art 144(a) Croatian Criminal Code; Maria Pawelec and Mateusz Łabuz, *Non-Consensual Sexualising Deepfakes - Threats and Recommendations for Legal and Societal Action*. (2025) CEE Digital Democracy Watch p18

²⁴ German Federal Council Drs. 222/24; Bundesrat 2024; Pawelec and Mateusz (n21)

²⁵ Kulturudvalget 2024-25 KUU Alm.del - Bilag 232 available at:

<https://www.ft.dk/samling/20241/almdel/kuu/bilag/232/3050901.pdf>; Dirk Visser, Deepfakes onder een naburing recht, *Mediaforum* 2024(5) (2024) pp.138-40

²⁶ Bernt Hugenholtz, "Deepfake Bills in Denmark and the Netherlands: Right idea, wrong legal framework", *Kluwer Copyright Blog* (august 6 2025) available at: <https://legalblogs.wolterskluwer.com/copyright-blog/deepfake-bills-in-denmark-and-the-netherlands-right-idea-wrong-legal-framework/>; Sofia Karttunen, *The Danish approach to copyright and deepfakes: A model for the EU?*, EPRS (January 2026)

²⁷; Amelia Nieremberg, "Denmark Aims to Use Copyright Law to Protect People From Deepfakes", *New York Times* (10 July 2025) available at: <https://www.nytimes.com/2025/07/10/world/europe/denmark-deepfake-copyright-ai-law.html>

²⁸ See e.g. Vincenzo Iaia, "To Be, or Not to Be ... Original Under Copyright Law, That Is (One of) the Main Questions Concerning AI-Produced Works", *71 GRUR International*, 793–812 (2022); Eleonora Rosati, "Copyright as an Obstacle or an Enabler? A European Perspective on Text and Data Mining and its Role in the Development of AI Creativity", *27 Asia Pacific Law Review* 198–217 (2019); Adam Buick, "Copyright and AI Training Data—Transparency to the Rescue?", *20 J. Intell. Prop. L. & Prac.* 182, 183 (2025); Thomas Margoni and Martin Kretschmer, "A Deeper Look into the EU Text and Data Mining Exceptions: Harmonisation, Data Ownership, and the Future of Technology", *71 GRUR Int'l* 685 (2022); Enrico Bonadio and Luke McDonagh, "Artificial Intelligence as Producer and Consumer of Copyright Works: Evaluating the Consequences of

At a high level, copyright law may be triggered in the creation of deepfakes in 4 principal ways. First, the use of pre-existing copyright-protected works as training data or prompts may constitute a copyright relevant and potentially infringing act (unless conducted with the rightsholder’s authorisation or subject to an exception and limitation).²⁹ Second, the resulting deepfake output may also infringe copyright where it reproduces the input’s protected original expression without the right holder’s authorisation or subject to an exception and limitation.³⁰ This operates independently of any rights or protections that may accrue to a depicted individual under other areas of law (e.g. personality rights). Third, the deepfake output may itself qualify for copyright protection where a human author exercises sufficient “free and creative choices”³¹ in the generative process.³² Such reasoning will apply irrespective of the nature of the deepfake, as copyright protection is not contingent on the legality or morality of the content.³³ Therefore, in principle, even non-consensual pornographic deepfakes could benefit from copyright protection.

While the above issues have been extensively debated by copyright scholars, often presenting diverging views³⁴, it is nevertheless clear that the creation of deepfakes implicates a layered rights landscape involving three distinct actors: the creator of the input work; the creator of the deepfake output and the individual depicted. While both the input and output creators may hold property rights under copyright law (provided they meet the required originality threshold³⁵), the depicted individuals will generally not receive any property rights over their likeness under copyright law.³⁶ This follows from the foundational principle that copyright only protects the original expression in authorial works rather than mere facts or naturally occurring elements.³⁷ A person’s appearance, voice, or mannerisms therefore fall outside such scope. It should be noted that some national jurisdictions (e.g. Netherlands and Italy) grant rights to subjects in copyright works within national copyright frameworks to accommodate fundamental

Algorithmic Creativity” *Intellectual Property Quarterly* 112-137 (2020); Peter Mezei, “You Ain’t Seen Nothing Yet” - Arguments against the Protectability of AI-generated Outputs by Copyright Law” In: Maurizio Borghi (eds.): *Informational Rights and Informational Wrongs: A Tapestry for Our Times*, 126-143 (2023)

²⁹ See e.g: Nicola Lucchi, *Generative AI and Copyright*, JURI Committee (2025); Kalpana Tyagi, “Deepfakes, Copyright and Personality Rights an Inter-Disciplinary Perspective” (2023). In: Mathis, K., Tor, A. (eds) *Law and Economics of the Digital Transformation*; Tim Dornis, Nicola Lucchi, “Generative AI and the Scope of EU Copyright Law: A Doctrinal Analysis in Light of the Referral in *Like Company v. Google*”. *IIC* 56, pp.1800–1840 (2025); Martin Kretschmer et al, “Copyright Law and the Lifecycle of Machine Learning Models”, *IIC* (2024) 55:pp.110–138

³⁰ See e.g. Eleonora Rosati, “Infringing AI: Liability for AI-Generated Outputs under International, EU, and UK Copyright Law.” *European Journal of Risk Regulation* 16, no. 2 (2025): pp.603–27; Tyagi (n29); Lucchi (n29); Bonadio and McDonagh (n28)

³¹ Case C-145/10 *Eva-Maria Painer v. Standard VerlagsGmbH et al.* ECLI:EU:C:2011:798 [88-89]; Case C-393/09 *Bepečnostní softwarová asociace – Svaz softwarové ochrany v. Ministerstvo kultury* ECLI:EU:C:2010:816 [28-42]; Case C-604/10 *Football Dataco Ltd et al. v. Yahoo! UK Ltd et al.* ECLI:EU:C:2012:115 [37-38].

³² See e.g. Bernt Hugenholtz and Joao Pedro Quintais, “Copyright and Artificial Creation: Does EU Copyright Law Protect AI-Assisted Output?”. *IIC* 52, 1190–1216 (2021); Andres Guadamuz, 'Do Androids Dream of Electric Copyright? Comparative Analysis of Originality in Artificial Intelligence Generated Works', in Lee and Liu (eds), *Artificial Intelligence and Intellectual Property* (2021); Iaia (n28); Lucchi (n29); Tyagi (n29); Mezei (n28)

³³ *ibid*

³⁴ See literature in n28, 29, 30, 32

³⁵ Case C-5/08 *Infopaq International A/S v Danske Dagblades Forening* ECLI:EU:C:2009:465 [37]

³⁶ Jennifer Rothman, “Copyrighting people”, *Journal of the Copyright Society* (2024); Jessica Lake, “Deepfake and non-consensual pornography: recent iterations of the gendered battle for rights in a photograph” in Jessica C Lai and Kathy Bowrey (eds) *A Research Agenda for Intellectual Property Law and Gender* (2025); Tyagi (n29)

³⁷ *ibid*

rights concerns.³⁸ The interests of the depicted individual are however more ordinarily protected through personality rights, privacy and data protection law, functioning rather as external limits on copyright.³⁹ Because the copyright owner of the work and the person depicted will rarely coincide, tensions arise between copyright and such frameworks, often requiring courts to balance the property interests of right holders against the fundamental rights of the individuals portrayed.⁴⁰ Within this context, it becomes evident that copyright infringement offers a potential ground for enforcement against the creation and dissemination of deepfakes. However, such recourse would only be available to the copyright owner of the infringed work, and/or the owner of the deepfake work. As these rightsholders are unlikely to coincide with the depicted individual, copyright law is inadequate in addressing the core issue arising from deepfakes: the harms experienced by the person depicted.

3. AMENDING COPYRIGHT LAW: THE DANISH AND DUTCH PROPOSALS

The above analysis has revealed that, while copyright law applies to multiple stages of the deepfake creation process, it largely fails to protect the interests of individuals depicted in deepfakes. It is precisely this gap that the recent Dutch and Danish proposals seemingly aim to address by granting individuals copyright protection over their likeness in digital reproductions. The Dutch initiative originates with Dutch VVD MP Rosemarijn Dral, drawing from a 2024 academic article by intellectual property scholar Dirk Visser.⁴¹ Further questions on this matter were additionally submitted to the cabinet by 4 members of House of Representatives.⁴² Similarly, the Danish proposal was formally submitted for consultation on July 7th 2025, with deliberations and potential implementation scheduled for Winter 2025/26.⁴³ While adopting comparable approaches, the wording and rights granted by both bills differs on some formal aspects.

Under the Danish proposal, amendments would be implemented in the Neighbouring Rights Act. Performers would receive an additional right over the making available to the public of “realistic digitally generated imitations of a performer or artist’s artistic performance”.⁴⁴ Such right would only extend to citizens and residents of EEA countries.⁴⁵ In addition, all individuals (including foreign nationals) would be granted rights over digitally-generated imitations of personal characteristics, prohibiting making available to the public of “realistic digitally generated imitations of a physical person’s personal, physical characteristics”.⁴⁶ Such right however remains subject to limitations for “caricature, satire, parody, pastiche, criticism of power, social criticism or the like”, unless the imitation

³⁸ Tatiana Synodinou, “Image Right and Copyright Law in Europe: Divergences and Convergences”

Laws (2014), 3(2) see e.g. Art 96-7 Italian Copyright Act; Art 21 Dutch Copyright Act

³⁹ Synodinou (n38) p.184

⁴⁰ Tyagi (n29); Synodinou (n38); Tyler Ochoa ‘Overlaps Between Copyright, Rights of Publicity, and Personality Rights’, in Neil Wilkof, Shammad Basheer, and Irene Calboli (eds), *Overlapping Intellectual Property Rights* (2023)

⁴¹ Visser 2024 (n25); Hicham Abarkan, “Kamer wil burgers auteursrecht geven op gezicht en stem: David versus Goliath?”, *Nos Nieuws* (15 July 2025)

⁴² In September 2025 the Cabinet confirmed Dutch law already offers a wide range of instruments to sufficiently address non-consensual deepfakes. See: Marjolein van Trigt, “Geen auteursrecht op uiterlijk en stem”, *BinnenlandsBestuur*, (22 September 2025) available at: <https://www.binnenlandsbestuur.nl/juridisch/geen-auteursrecht-op-uiterlijk-en-stem>

⁴³ Kulturudvalget (n25) ; Nieremberg (n27)

⁴⁴ Section 65a(1) proposed amendments to Danish Neighbouring Rights Act . Translation by Dirk Visser in “*The Dutch and Danish proposals for legislation on deepfakes*”, *ItenRecht* (2025)

<https://www.itenrecht.nl/artikelen/the-dutch-and-danish-proposals-for-legislation-on-deepfakes>

⁴⁵ Section 86(2) proposed amendments to Danish Neighbouring Rights Act translation by Visser (n44)

⁴⁶ Section 73a(1) proposed amendments to Danish Neighbouring Rights Act translation by Visser (n44)

would constitute misinformation in a manner that would seriously harm other's fundamental rights and interest.⁴⁷ Both rights would subsist for 50 years from the performer/individual's death.⁴⁸

The Dutch proposal similarly aims to grant all individuals an exclusive right to create, reproduce, distribute, broadcast, make available, or disclose a deepfake with their likeness.⁴⁹ The definition of a deepfake follows that of Art 3(60) AIA: "an AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful."⁵⁰ Compared to the Danish proposal, the Dutch amendments provide more detailed rules on transferability, licensing and post-mortem exercise of the rights. The right would subsist for 70 years after an individual's death.⁵¹ It is non-transferrable upon succession and not subject to attachment.⁵² An exception applies where a deepfake is produced with the depicted individual's consent for a film or phonogram.⁵³ Licensing is permitted, however, where an exclusive license is granted, the individual retains the right to object to deepfakes harming their honour or reputation.⁵⁴ All existing limitations, including caricature parody and pastiche, would apply to the exercise of this right.⁵⁵

Despite their formal differences in wording and scope, both proposals converge at their core, establishing a new right for individuals over their likeness in digital reproductions. These initiatives reflect growing concerns that existing legal frameworks may be insufficient in combating deepfakes and their associated harms. Despite increased endorsement by the Danish Media Council for Children and Young People⁵⁶ and Danish Lawyers Association⁵⁷, it is necessary to assess whether the proposed amendments to Dutch and Danish copyright law address a genuine regulatory gap and can provide effective redress for non-consensual deepfake victims. In particular, it should be examined whether existing legal frameworks already provide adequate protection against unauthorised digital reproductions of individuals' likenesses, or whether deepfake technology exposes limitations that justify legislative intervention. The following sections will address these questions.

4. REGULATING DEEPPAKES IN THE EU

To fully assess whether amendments to Danish and Dutch copyright law are necessary and effective, one must first examine how deepfakes are currently regulated in the EU and the respective national jurisdictions. The regulation of deepfakes currently operates within a fragmented legal landscape, where a variety of legal domains may be implicated depending on the nature of the content. Victims of non-consensual deepfakes may seek redress through several grounds, including (but not limited to) fundamental rights, data protection, personality/publicity rights, competition and consumer law, and

⁴⁷ Section 73a(2) proposed amendments to Danish Neighbouring Rights Act translation by Visser (n44)

⁴⁸ Section 73a(3); Section 65a(2) proposed amendments to Danish Neighbouring Rights Act translation by Visser (n44)

⁴⁹ Section 7C proposed amendments to Dutch Copyright Act Translation by Visser (n44)

⁵⁰ Section 1(w) proposed amendments to Dutch Copyright Act Translation by Visser (n44)

⁵¹ Section 12(8) proposed amendments to Dutch Copyright Act Translation by Visser (n44)

⁵² Section 9(4-6) proposed amendments to Dutch Copyright Act Translation by Visser (n44)

⁵³ Section 9(6) proposed amendments to Dutch Copyright Act Translation by Visser (n44)

⁵⁴ Section 9 (4-6) proposed amendments to Dutch Copyright Act Translation by Visser (n44)

⁵⁵ Section 10 proposed amendments to Dutch Copyright Act Translation by Visser (n44)

⁵⁶ Medieradet for Born & Unge, *Høring over udkast til lov om ændring af lov om ophavsret (Indførelse af en præstationsbeskyttelse og beskyttelse mod digitalt genererede efterligninger mv.)* (20 August 2025) available at: <https://cdn.medieraadet.dk/medieraadet/Media/638912879296441026/Medier%C3%A5det%h%C3%B8ringssvar%j%C3%A6ndring%2025.pdf>

⁵⁷ Danske Advokater, *Høringssvar over forslag til lov om ændring af lov om ophavsret (Indførelse af en præstationsbeskyttelse og beskyttelse mod digitalt genererede efterligninger mv.)* (20 August 2025) available at: <https://www.datocms-assets.com/143970/1755772367-200825ophav.pdf>

criminal law.⁵⁸ These regimes constitute a broad patchwork of legal frameworks that, while not specifically designed to address deepfakes, may nonetheless offer enforcement avenues.⁵⁹ Alongside these general frameworks, EU law has introduced specific measures directly targeting specific forms of deepfake media: the AIA, DSA and GBVD.⁶⁰ The following section will briefly map the main legal frameworks applicable to deepfakes in the EU, highlighting gaps or limitations. This analysis provides the foundation to evaluate the Danish and Dutch proposed copyright amendments in Section 5 below. Due to the broad range of legal frameworks potentially implicated by deepfakes at both national and EU level, a comprehensive analysis remains outside the scope of the present paper. The analysis below is rather confined to the main frameworks/instruments available for victims to seek redress and enforcement.

A. AI Act

The AIA constitutes the first framework for regulating the development and deployment of AI systems in the EU. It adopts a risk-based approach, imposing obligations for both providers and deployers according to 4 categories of risk: minimal, limited, high risk and prohibited practices.⁶¹ Despite significant controversy⁶², deepfake technologies are classified as limited risk AI systems and are thus solely subject to the transparency obligations of Art 50 AIA.⁶³ Art 50(2) AIA requires providers of AI systems generating synthetic media to ensure that any artificially generated or manipulated content is appropriately disclosed as such, while Art 50(4) AIA imposes the same obligation on deployers of AI systems. Two important limitations however apply. Art 50(4) AIA clarifies that, in the case of artistic, creative, satirical and fictional content, the disclosure requirement must not hamper the display and enjoyment of the work. Furthermore, reading Art 3(4) AIA in conjunction with Art 50 AIA, a household exemption would apply to deployers of AI systems pursuing a purely personal activity, exempting them from the transparency obligations.

Scholarship has highlighted a number of uncertainties and unresolved issues in regards to the practical implementation of the Art 50 AIA obligations. Amongst the principal concerns are the broad and ambiguous scope of the “manipulated image” definition,⁶⁴ the nature of the required disclosure,⁶⁵ and misalignment between providers’ and deployers’ obligations.⁶⁶ However, more fundamentally for the purpose of the present discussion, the AIA transparency obligations only address deepfakes’ risks of deception and misinformation.⁶⁷ In particular, it overlooks the significant issue of sexually explicit and intimate deepfakes.⁶⁸ This is a key omission considering such type of material constitutes the overwhelming majority of deepfakes circulating online.⁶⁹ The Art 50 AIA obligations offer no redress or real protection from the psychological and reputational harms inflicted by such type of content on

⁵⁸ Krack (n7)

⁵⁹ *ibid*

⁶⁰ *ibid*

⁶¹ Recital 26 AIA ; Krack (n7)

⁶² See e.g Mateusz Labuz, ‘Regulating Deepfakes in the Artificial Intelligence Act’, 2 *Applied Cybersecurity & Internet Governance* (2023)

⁶³ Labuz (n62); Krack (n7) p.346

⁶⁴ Van der sloot *Regulating the Synthetic Society Generative AI, Legal Questions and Societal Challenges* (2024)

⁶⁵ *ibid*

⁶⁶ Martina J Block, “A Critical Evaluation of Deepfake Regulation through the AI Act in the European Union” 13 *Journal of European Consumer and Market Law*, (2024)

⁶⁷ Krack (n7)

⁶⁸ Labuz (n62); Felipe Romero Moreno, “Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content” *International Review of Law, Computers & Technology* (2024); Krack (n7) p.349

⁶⁹ Ajder H. et al (n15); The Home Security Heroes (n15)

victims. As noted by Block, merely indicating that content has been manipulated will unlikely alleviate the psychological harms experienced by a victim of non-consensual deepfake pornography.⁷⁰

Ultimately, the AI act is primarily oriented towards safeguarding the general public from deception and misinformation, rather than protecting individuals' whose likeness is used in deepfakes. As such, it only offers a limited response to the core challenges and harms posed by deepfake technology.

B. GBVD

The GBVD harmonises the criminalisation of various forms of violence against women, establishing minimum rules across the EU. In doing so, it addresses several shortcomings of the AIA with respect to non-consensual sexually explicit and intimate deepfakes, and seeks to remedy gaps in national criminal laws.⁷¹ Art 5(1)(b) GBVD criminalises with up to 1 year of imprisonment, the production, manipulation, alteration and subsequent dissemination of material falsely depicting individuals in sexually explicit activities without a person's consent, when likely to cause the victim serious harm. Recital 19 GBVD clarifies "images, photographs and videos, including sexualised images, audio clips and video clips" are included in such type of prohibited material. Art 5(2) GBVD however reaffirms that the provision shall not prejudice the fundamental rights of freedom of expression and information and freedom of the arts.

While Art 5(1)(b) GBVD clearly encompasses deepfakes depicting individuals in sexually explicit activities, its scope is limited in several aspects. First, it likely will not cover non sexually explicit intimate deepfakes (e.g. nude photos or videos), which may nonetheless severely harm victims.⁷² A second factor limiting the provision's scope concerns the meaning of "making accessible to the public".⁷³ Recital 18 GBVD provides little interpretative guidance, merely stating it should be understood as "potentially reaching a number of persons". Scholarship has suggested that a literal dictionary interpretation of the term "a number of" would imply a minimum of over 3 people.⁷⁴ This would potentially exclude instances in which the material is shared in closed or private contexts (e.g. direct private messaging from a user to another or in small private groups), despite this being amongst the most common modes of dissemination of such material.⁷⁵ The interpretative uncertainty is further compounded by the different formulation of "public dissemination" as related to cyber incitement to violence adopted in Recital 26 GBVD.⁷⁶ In such context, public dissemination is defined as making material accessible to a potentially unlimited number of persons or to users in general, thus presupposing an even larger scale of dissemination required.⁷⁷ The remaining ambiguity leaves considerable room for divergent interpretations by Member States in transposing the directive and national courts in applying the provisions.⁷⁸ Finally, the requirement that the conduct be likely to inflict "serious harm" further restricts the provision's applicability.⁷⁹ It imposes an additional burden of proof on the victim and leaves

⁷⁰ Block (n66); Krack (n7)

⁷¹ Can Yavuz, "Criminalisation of the Dissemination of Non-Consensual Sexual Deepfakes in the EU. A Comparative Legal Analysis" (2024) 95 *RIDP*; *European Commission Commission Staff Working Document*

⁷² Yavuz (n71); Krack (n7) p.351

⁷³ *ibid*

⁷⁴ *ibid*

⁷⁵ Sofie Royer et al, "An Empirical and Legal Analysis of Sexual Deepfakes in the EU, Belgium and the Netherlands" (2024) 95 *RIDP* p.459-65

⁷⁶ Krack (n7) p351

⁷⁷ *ibid*

⁷⁸ *ibid*

⁷⁹ Krack (n7) p351; European Women's Lobby, "Report on Cyber Violence Against Women" (September 2024), <https://www.womenlobby.org/NEW-PUBLICATION-Report-on-Cyber-Violence-Against-Women>

considerable discretion to national courts in determining what shall constitute “serious harm”, potentially leading to divergences across Member States.⁸⁰

While the GBVD addresses some of the AIA’s shortcomings concerning sexually explicit deepfakes, it only offers victims limited legal recourse under circumscribed conditions. Significant categories of harmful deepfakes, such as intimate and political deepfakes, remain outside its scope. Additionally, key ambiguities raise the risk of inconsistent application across Member States, potentially undermining the protection offered to victims.

C. DSA

Building upon and revising the E-Commerce directive, the DSA constitutes a key component of the EU regulatory framework for digital services, providing accountability and liability rules for intermediary services. Focusing on content moderation and platform accountability, the DSA plays a key role in the enforcement for victims of deepfakes.⁸¹ In seeking to balance freedom of expression with the need to protect individuals online, the DSA primarily targets illegal content, while additionally imposing obligations on Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) with respect to harmful content.⁸²

While the Regulation does not provide a detailed definition of “illegal content”, Art 3(h) DSA broadly defines it as “any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any Member State which is in compliance with Union law”. Recital 12 DSA lists amongst examples of such type of content the unlawful non-consensual sharing of private images and the unauthorised use of copyright protected material, both relevant in the context of deepfakes. On the basis of these definitions, certain types of deepfakes will clearly fall within the scope of illegal content. In particular, due to their criminalisation under the GBVD, non-consensual sexually explicit deepfakes would be considered illegal content.⁸³ Per Recital 12, copyright infringing deepfakes would similarly be deemed illegal. In theory, copyright could therefore serve as a ground for enforcement under the DSA for a broad range of deepfakes, irrespective of the specific nature of the content. In practice, however, the copyright owner of the underlying input material will typically be a third party rather than the depicted individual. The status of other types of deepfake content remains more complex to assess and will require a case-by-case examination. Nevertheless, as will be discussed in Sections D and E below, deepfakes may infringe data protection, privacy law, and personality rights of individuals depicted, thus providing an alternative basis to consider other forms of deepfakes (beyond non-consensual sexually explicit ones) illegal.

With respect to illegal content, the DSA establishes a clear and detailed framework governing platforms accountability and liability.⁸⁴ Per Art 6 DSA, hosting providers will be liable for users’ illegal content when they have actual knowledge or fail to swiftly remove/disable access to the illegal content upon receiving actual knowledge. User notices or law enforcement orders shall be considered to grant actual knowledge.⁸⁵ Such measure is key in curbing the dissemination of non-consensual deepfakes for victims, providing strong incentives for platforms to ensure swift removals to avoid liability and fines. Chapter

⁸⁰ *ibid*

⁸¹ Anastasia Karagianni, and Miriam Doh, “A Feminist Legal Analysis of Non-Consensual Sexualized Deepfakes: Contextualizing Its Impact as AI-Generated Image-Based Violence under EU Law.” *Porn Studies, November*, pp.1–18 (2024); van Huijstee et al (n13); Krack (n7)

⁸² Martin Husovec, *Principles of the Digital Services Act* (2024) pp.19-32

⁸³ Art 5(1)(b) GBVD. For further discussion on the intersection of the DSA and GBVD see Krack (n7)

⁸⁴ Husovec (n82)

⁸⁵ Recital 22 DSA

III DSA further sets out a series of due diligence obligations applicable to all intermediary services, with specific obligations for hosting services, online platforms, platforms allowing consumers to conclude distance contracts with traders, and VLOPS/VLOSES. A detailed examination these obligations falls beyond the scope of the present paper, and has been widely addressed by existing literature.⁸⁶ Two obligations are however particularly relevant in the context of deepfakes: the requirement that hosting providers implement notice and action mechanisms enabling users to report illegal content⁸⁷, and the requirement to provide a statement of reason to affected users following content moderation decisions.⁸⁸ Articles 34 and 35 DSA impose further obligations on VLOPs and VLOSEs, requiring them to assess and mitigate systemic risks posed by their services. Systemic risk encompasses the dissemination of illegal content, negative effects on fundamental rights, civic discourse, public security, gender based violence or a personal wellbeing.⁸⁹ This framework therefore would cover non-consensual sexually explicit deepfakes, alongside other forms of harmful deepfakes depicting individuals without their consent (e.g. political deepfakes).⁹⁰

As the rapid online dissemination of deepfakes significantly exacerbates the harms to individuals, amplifying exposure, reputational damage and psychological impacts, the ability to secure swift removal is crucial for victims.⁹¹ In this regard, the DSA provisions can, in principle, contribute to combating deepfakes and their associated risks/harms. However, the DSA merely harmonises procedural aspects of content moderation, and in practice may not be able to guarantee effective enforcement. Swift removal may not always be secured due to the volume of requests to be processed by platforms, and even when content is removed, it may rapidly reappear and proliferate across other platforms as users are able to download save and reupload material.⁹²

3.D. Personality Rights

Personality rights may provide a further key legal basis to protect victims from non-consensual deepfakes. As no harmonised framework of personality rights exists at EU level, protection remains highly fragmented and regulated at national level.⁹³ Across Member States, personality rights derive from a range of statutory bases, including constitution, tort law, criminal law, statute and case law.⁹⁴ National jurisdictions however broadly converge in their protection of privacy, dignity, honour, and reputation.⁹⁵ As such, personality rights will commonly encompass the right to one's image, granting individuals control over how aspects of their image/likeness are used by others.⁹⁶ Depending on the national framework, such rights shall encompass patrimonial and non-patrimonial aspects.⁹⁷

⁸⁶ See e.g. Husovec (n82)

⁸⁷ Art 16(1) DSA

⁸⁸ Art 17 DSA

⁸⁹ Art 34(1)(a)-(d) DSA

⁹⁰ Krack (n7) p.356

⁹¹ Karagianni and Doh (n81); Krack (n7); Ajder et al (n15); Royer et al (n75)

⁹² *ibid*

⁹³ Synodinou (n38); Gert Brüggemeier et al. "A Common Core of Personality Protection." In *Personality Rights in European Tort Law*, Brüggemeier et al (eds) pp. 567–77 (2010); Gert Brüggemeier, "Protection of Personality Rights in the Law of Delict/Torts in Europe: Mapping out Paradigms." *Personality Rights in European Tort Law*, Brüggemeier et al (eds) pp.5–37 (2010); Eva Ondreasova, "Personality Rights in Different European Legal Systems: Privacy, Dignity, Honour and Reputation", in Oliphant et al (eds) *The Legal Protection of Personality rights: Chinese and European Perspective* (2018) pp.24-70

⁹⁴ *ibid*

⁹⁵ *ibid*

⁹⁶ *ibid*

⁹⁷ *ibid*

The creation of deepfakes may implicate personality rights, as the generated output may appropriate, reproduce or manipulate an individual's likeness (face, voice, or other distinctive features). While non-consensual sexually explicit deepfakes constitute the most severe and intrusive violations of personality rights, other types of deepfakes (e.g. ones portraying individuals participating in unlawful activities) may nonetheless substantially harm individual's honour, reputation, and dignity. In light of the fragmented and national character of personality rights across Europe, the present analysis shall not provide a comprehensive mapping of all Member States. Instead, it will present the principal features of personality rights in Denmark and the Netherlands, as relevant to evaluate the necessity and adequacy of the proposed copyright-based interventions.

In Denmark, aspects of personality rights are protected through Chapters 26 and 27 of the Danish Penal Code, which regulate offences against personal liberty, personal honor and certain individual rights.⁹⁸ In addition to these non-patrimonial aspects of personality rights, generally protected through the right of privacy, Danish law also recognises a patrimonial dimension through the right of publicity.⁹⁹ While not codified in a standalone statutory provision, it constitutes an established legal principle in case law and general provisions of the Danish Marketing Practices Act.¹⁰⁰ Importantly, the right applies to all individuals irrespective of whether they commercially exploit their identity, and can be licensed.¹⁰¹ As a general requirement, for infringement to occur, an individual must be identifiable.¹⁰² This would exclude small formats, poor quality images, or rapid sequences where the image is not visible for long enough to enable identification.¹⁰³ The rough sketch of handball players in an online fantasy sports game was found insufficiently recognisable; however the court noted that the addition of more distinctive personal features would have triggered personality rights protection.¹⁰⁴ Danish courts additionally apply a necessity criterion when assessing infringement.¹⁰⁵ Necessity is to be understood in light of how intrusive the use of a person's likeness is.¹⁰⁶ In the handball player's online game case, the use of players' names to accompany the rough sketches was held necessary and natural for the functioning of the game, and thus not infringing.¹⁰⁷

Similarly, in the Netherlands, courts have recognised personality rights through a flexible and broad interpretation of Section 21 Dutch Copyright Act.¹⁰⁸ Section 21 Dutch Copyright Act prohibits the disclosure by the rightsholder of portraits not made on commission if there is a reasonable interest for disclosure on the part of the person depicted. Per the Explanatory Memorandum to the Act, portraits are representations depicting an individual (whether including other body parts or not).¹⁰⁹ Courts have interpreted this broadly, encompassing any depiction in which the person is recognisable to others,

⁹⁸ Law Business Research Report, *Right of Publicity* (2017) pp. 22-26; Thomas Riis, "The Use of Personal Characteristics in Sports Managers Games" in *Intellectual Property and Sports: Essays in Honour of P. Bernt Hugenholtz*, Martin Senftleben et al (eds) pp.107-16

⁹⁹ *ibid*

¹⁰⁰ *ibid*

¹⁰¹ *ibid*

¹⁰² *ibid*

¹⁰³ *ibid*

¹⁰⁴ Ugeskrift for Retsvæsen 2015.2936 Ø.; Riis (n98)

¹⁰⁵ *ibid*

¹⁰⁶ *ibid*

¹⁰⁷ *ibid*

¹⁰⁸ Riis (n98); Synodinou (n38); Kian Hsia and Thijs van den Heuvel, "Levelling the playing field in eSports – Dutch portrait rights in games", *Interactive Entertainment Law Review* (2018) pp.67-70

¹⁰⁹ Hsia and van den Heuvel (n108);

regardless of whether the face is visible.¹¹⁰ The reasonable interest requirement has been interpreted by courts as including two dimensions: a non-patrimonial one related to privacy and a commercial interest.¹¹¹ Privacy is recognised as a reasonable interest for enforcement under Section 21 Dutch Copyright Act, allowing anyone whether famous or not, to oppose publication of a portrait if seriously harming their privacy, subject to balancing with Art 8 and 10 ECHR.¹¹² In conducting such an assessment, factors taken into account by courts include the specific circumstances in which the picture is created, nature of the picture, the nature/intimacy in which the person is depicted, publication context, correctness of any accompanying information to the image, public interest or informative value of the publication.¹¹³ The second dimension of reasonable interest concerns commercial interest, protecting against the commercial exploitation of one's image without consent.¹¹⁴ It exclusively applies where an individual has sufficient fame to give rise to commercial exploitation of their image.¹¹⁵ Such interest is however to be balanced against freedom of expression¹¹⁶, with the assessment taking into account the informative value of the publication alongside the nature of the portrait and publication.¹¹⁷

The Dutch courts have applied and interpreted Art 21 Dutch Copyright Act portrait rights flexibly.¹¹⁸ In the *Edgar Davids* case, the court found that the use of the “Striker skin” feature in popular online game League of Legends violated Dutch footballer Edgar Davids’ portrait rights.¹¹⁹ The digital avatar’s dark skin, black dreadlocks, black sporting glasses and uniform, along with its aggressive playing style, were considered sufficiently distinctive to make Davids identifiable.¹²⁰ The court additionally dismissed the defendant’s Art 10 ECHR arguments, finding Davids’ reasonable interest in opposing use of his image without compensation outweighed the gaming company’s freedom of expression.¹²¹ In the 2022 *Max Verstappen* judgement, the Supreme Court further expanded the scope of portrait rights, holding that even an image of a lookalike may, when identifying an individual, be considered a portrait for the purposes of Art 21 Dutch Copyright Act.¹²² Courts are to consider factors such as how the lookalike is depicted (e.g. specific makeup or clothing), other elements included, and the context in which the image is shared.¹²³ While the intended character of the image (e.g. parody) is not determinative in establishing whether a depiction shall be classified as a portrait, it shall play a role in balancing the interests at stake and assessing reasonable interest.¹²⁴ In considering such factors, the Supreme court held an

¹¹⁰ See *Netherlands Supreme Court, ECLI:NL:HR:1987:AD0034, para 3.2; Netherlands Supreme Court, ECLI:NL:HR:2003:AF3416, para 4.6.3 Dutch Supreme Court, 30 October 1987, NJ 1988, 277 (Naturiste); Dutch Supreme Court, 2 May 2003, NJ 2004, 80 (Nielsen & IPA/Storms Factory;Breekijzer).*

¹¹¹ Hsia and van den Heuvel (n108);

¹¹² Hsia and van den Heuvel (n108); Dutch Supreme Court, 21 January 1994, NJ 1994,473 (*Moordenaar G.J. Heijn*).

¹¹³ Hsia and van den Heuvel (n108); Dutch Supreme Court, 1 July 1998, ECLI:NL:HR:1988:AB7688 (*Vondelpark*); Dutch Supreme Court, 14 June 2013, ECLI:NL:HR:2013:CA2788 (*Cruiff/ Tirion*).

¹¹⁴ Hsia and van den Heuvel (n108)

¹¹⁵ *ibid*

¹¹⁶ Art 10 ECHR

¹¹⁷ Hsia and van den Heuvel (n108)

¹¹⁸ *ibid*

¹¹⁹ District Court Amsterdam, 9 August 2017, ECLI:NL:RBAMS:2017:5415 (*Edgar Davids v Riot Games*).

¹²⁰ *ibid*

¹²¹ *ibid*

¹²² Dutch Supreme Court 22 April 2022, ECLI:NL:HR:2022:621 (*Verstappen v PICNIC*); Headnotes by Editorial Board, “A Lookalike Can Amount to a Portrait under the Copyright Act”, *GRUR International*, Volume 71, Issue 12, (2022) pp.1218–1220

¹²³ *ibid*

¹²⁴ *ibid*

advertisement including a lookalike of Dutch F1 driver Max Verstappen sufficiently identified him and thereby constituted a portrait per Art 21 Dutch Copyright Act.¹²⁵

Despite doctrinal differences, both Danish and Dutch personality rights frameworks both already offer adequate legal protection to victims of non-consensual deepfakes. The broad interpretation of a “portrait” under Art 21 Dutch Copyright Act would likely encompass most forms of deepfakes reproducing an individual’s likeness, and even deepfakes only incorporating distinctive features identifying the individual (as illustrated in *Edgar Davids*¹²⁶ and *Max Verstappen*¹²⁷). While only well-known individuals, victims of deepfakes, will be able to pursue an action based on commercial interest, all victims may invoke privacy interests. These rights must however be balanced against freedom of expression alongside the potential copyright interests of the deepfake creator. In cases involving non-consensual sexually explicit deepfakes, the victim’s personality rights will be more likely to prevail, whereas creative and parodic deepfakes may shift the balance in favour of the creator’s freedom of expression. Similarly, under Danish law, victims of deepfakes may rely on personality rights interests for enforcement, provided the individual depicted is identifiable. Importantly, unlike the Netherlands, all individuals would be able to pursue both privacy and publicity interests, without the need to prove commercial exploitability of one’s image. Both famous and non-famous individuals will therefore be able to enforce both patrimonial and non-patrimonial aspects.

Cross-cutting issues can however be identified in both jurisdictions. The identifiability requirement, central to both systems, may be straightforward to apply in the context of deepfakes appropriating entire appearances or distinctive features. Its application may however be more complex in nuanced situations, such as where less distinctive features of multiple individuals are combined to create new fictional persons.¹²⁸ In such cases, no single identifiable individual would be depicted, thus personality rights may not apply.¹²⁹ Similar concerns may arise in regards to stylised depictions. A secondary issue concerns enforcement and mitigation of harms for victims. While personality rights provide an avenue for legal action, orders for removal of content by a court may not necessarily prevent the rapid re-uploading and dissemination of content across other platforms by third parties.¹³⁰ As previously noted, deepfakes spread rapidly, and damages awards are unlikely to meaningfully compensate for the severe psychological and reputational harms victims may experience. As a result, enforcement and mitigation of harms may remain an issue for victims.

E. Privacy and Data Protection Law

The creation and dissemination of deepfakes depicting individuals will finally also broadly implicate the right to privacy and data protection¹³¹. Relevant literature has explored these implications in depth.¹³² Most notably, the creation and dissemination of deepfakes depicting real individuals will trigger the

¹²⁵ Ibid; The question of whether Verstappen had reasonable interest in opposing the public depiction was however remanded to the *hof den haag* court for further assessment.

¹²⁶ *Edgar Davids v Riot Games* (n119)

¹²⁷ *Verstappen v PICNIC* (n122)

¹²⁸ Tyagi (n29)

¹²⁹ *ibid*

¹³⁰ *ibid*

¹³¹ Art 8 ECHR; Art 7-8 CFR

¹³² See e.g. Bart van der Sloot and Yvette Wagenveld, ‘Deepfakes: regulatory challenges for the synthetic society’ *Computer Law & Security Review Vol 46* (2022); Alessia Zornetta and Ignacio Cofone, ‘Artificial Intelligence and the Right to Privacy’, in Jeroen Temperman, and Alberto Quintavalla (eds), *Artificial Intelligence and Human Rights* (2023); Moreno (n68); Huijstee et al (n81)

application of the General Data Protection Regulation (GDPR).¹³³ The GDPR imposes strict rules on the collection and processing of personal data, defined under Art 4(1) GDPR as any information relating to an identified or identifiable natural person. Processing is broadly defined in Art 4(2) GDPR as “any operation performed on personal data, including collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available”. Use of Images, video recordings and voice recordings of real individuals in training data as input to a deepfake or incorporated into the deepfake output would therefore fall within the GDPR’s definition of personal data processing, thus triggering the application of the GDPR rules.¹³⁴

Art 5 GDPR lays down principles for data controllers in regards to data processing. Per Art 6 GDPR, the processing of personal data requires a lawful basis, listed in Art 6(1)(a)-(f) GDPR. In regards to the creation and dissemination of deepfakes, consent and legitimate interest offer the most relevant potential grounds for lawfulness of processing under the GDPR.¹³⁵ As the present discussion focuses on non-consensual deepfakes, consent will not be relevant in this context. Legitimate interest could offer an alternative avenue for data controllers to claim lawful processing of personal data. However, such basis requires a balancing test between controller’s interests and the data subject’s fundamental rights and freedoms.¹³⁶ Given the intrusive, explicit and harmful nature of most deepfakes disseminated online, it is unlikely that a legitimate interest claim could prevail beyond the narrowly confined contexts of deepfakes generated for parodies, artistic expression or journalistic activity.¹³⁷ Even in such cases a proportionality assessment would be conducted.¹³⁸ Accordingly, in the absence of a valid lawful basis, the creation and dissemination of deepfakes including real individuals’ personal data in the input or output would likely constitute prohibited unlawful processing under the GDPR.¹³⁹

Despite its broad scope, the application of the GDPR to deepfakes raises several unresolved issues. It should first be noted that the GDPR only protects living individuals; thus the processing of images, video and voice recordings of deceased persons will fall outside its scope.¹⁴⁰ Additionally, the Art 2(2)(c) GDPR household exemption, specifying the Regulation shall not apply to natural persons in the course of a purely personal or household activity, may provide an unintentional avenue to avoid liability for individuals in specific online contexts.¹⁴¹ Explicatively, the application of the household exemption remains unclear in contexts of online dissemination of deepfakes by private individual for non-commercial purposes.¹⁴² This may include sharing a deepfake with a small group of friends, through instant direct messaging between private users, or posting a deepfake within a “private” online group or closed social-media space. Despite the lack of specific guidelines on the topic, the CJEU’s and Working

¹³³ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

¹³⁴ Moreno (n68); Huijstee et al (n81)

¹³⁵ Art 6(1)(a) GDPR; Art 6(1)(f)

¹³⁶ Moreno (n68); Huijstee et al (n81)

¹³⁷ *ibid*

¹³⁸ *ibid*

¹³⁹ *ibid*

¹⁴⁰ van der Sloot and Wagenveld (n132)

¹⁴¹ *ibid*

¹⁴² *ibid*

Party 29's narrow interpretation of the household exemption¹⁴³ suggests that, once a deepfake is shared outside the strictly personal sphere, the exemption will generally no longer apply.¹⁴⁴

Ultimately, despite some outstanding uncertainties that remain to be clarified, the GDPR provides strict rules for data controllers and rights for data subjects that will apply to the creation and dissemination of deepfakes and enable legal action for victims.

5. COPYRIGHT LAW AS A TOOL TO COMBAT NON-CONSENSUAL DEEPFAKES?

As mapped in Section 4 above, a wide array of legal instruments are already available to victims of non-consensual deepfakes at both national and EU level. In particular, national personality rights regimes in the Netherlands and Denmark would appear to already offer a broad and adaptable framework for addressing non-consensual deepfakes, seemingly comparable to what put forth by the Danish and Dutch proposed copyright bills. Against this background, the question arises as to whether the proposed copyright law amendments would significantly enhance protection for victims. Would these amendments be effective in addressing non-consensual deepfakes' harms or would they rather introduce additional practical and enforcement issues? The following section will examine the potential benefits and drawbacks of the proposed amendments, with the aim of evaluating whether copyright law constitutes an appropriate framework for addressing non-consensual deepfakes.

A. Benefits

Situating the proposed Danish and Dutch rights within the framework of copyright and neighbouring rights could potentially streamline enforcement, particularly with regard to the rapid removal of deepfakes from online platforms. Copyright-infringing content uploaded is likely to be easier and faster for platforms to identify, as its unlawfulness may be less ambiguous and only require limited evidence. This assumption appears to be supported by a 2024 audit study examining the takedown speed of non-consensual intimate media on X in the US.¹⁴⁵ The study uploaded 50 AI generated nude images, reporting 25 for copyright infringement under the Digital Millennium Copyright Act (DMCA) and an identical set of 25 for violations of X's non-consensual nudity policy.¹⁴⁶ The study revealed that images reported on copyright grounds were removed within 25 hours at a 100% removal rate, while the same images reported for violating X's Terms & Conditions remained online for over 3 weeks with a 0% removal rate.¹⁴⁷

Perhaps regrettably, the study did not investigate the potential reasons underlying this substantial disparity between reporting systems. A comparable study conducted in the EU, particularly under the DSA framework, would have been valuable in further assessing the relevance of the above findings to the present discussion. A plausible explanation for the observed difference in removal rates may lie in the availability of elevated statutory damages for copyright infringement under US copyright law. Statutory damages for infringement range between 750\$ to 30,000\$ per work and reach up to 150,000\$ if the infringer's conduct is willful.¹⁴⁸ The prospect of such substantial payments is likely to create strong

¹⁴³ C-101/01 *Bodil Lindqvist* ECLI:EU:C:2003:596 (2003); C-212/13 *František Ryneš v Úřad pro ochranu osobních údajů*, ECLI:EU:C:2014:2428 (2014); Article 29 Data Protection Working Party, *Opinion 5/2009 on online social networking*, 01189/09/EN WP 163, (2009) van der Sloot and Wagenveld (n132)

¹⁴⁴ *ibid*

¹⁴⁵ Li Qiwei and others, "Reporting Non-Consensual Intimate Media: An Audit Study of Deepfakes" (arXiv, 2024)

¹⁴⁶ *ibid*

¹⁴⁷ *ibid*

¹⁴⁸ 17 U.S. Code § 504(c)(1)-(2)

incentives for platforms to ensure swift removals. By contrast, no statutory damages are available for breaches of platforms' non-consensual nudity policy in the US.

If statutory IP damages are indeed a key driver behind the swift removal of nude deepfakes reported for IP infringement in the US, this argument becomes more tenuous in the EU. Statutory damages for IP infringement are not available in the EU. Under the Intellectual Property Rights Enforcement Directive (IPRED)¹⁴⁹, courts may calculate damages by taking into account “all appropriate aspects, such as the negative economic consequences, including lost profits, which the injured party has suffered, any unfair profits made by the infringer and, in appropriate cases, elements other than economic factors, such as the moral prejudice caused to the rightsholder by the infringement”.¹⁵⁰ Alternatively damages may be set “as a lump sum on the basis of elements such as at least the amount of royalties or fees which would have been due if the infringer had requested authorisation to use the intellectual property right in question”.¹⁵¹ The CJEU has clarified that Member States may nonetheless additionally provide punitive damages under national law, however no Member State would appear to have adopted any such measure to date.¹⁵² Furthermore in the EU, nude deepfakes infringing a platform's Terms and Conditions are likely to fall within the broad category of “harmful content” under the DSA. Therefore, pursuant to Art 4-6 DSA, service providers may incur liability and fines where failing to expeditiously remove or disable access to the content. Accordingly, due to the lack of statutory damages in the EU and the DSA liability rules, divergences in removal rates described above would arguably be less pronounced if the study were to be repeated in the EU.

B. Drawbacks

While providing limited additional benefits, situating the proposed rights in the copyright and neighbouring rights framework may raise a number of practical and theoretical issues, which render potential adoption problematic.

Notwithstanding the formal expansion of rights for victims under the proposed bills, effective enforcement may in practice be undermined due to the inherent conflict between the territorial nature of copyright and the borderless nature of online dissemination of deepfakes.¹⁵³ Per Art 5 Berne Convention, and as restated by the CJEU in *Lagardère*, copyright is granted and enforced by each individual state in its own territory under national law.¹⁵⁴ Deepfakes, by contrast, (as most forms of content published online) are disseminated and accessible globally across multiple-jurisdictions (assuming no geo-blocking restrictions are in place). The risks and harms associated with deepfakes are therefore cross-border and global in nature.¹⁵⁵ As such, national copyright regimes provide an ill-suited instrument to effectively provide redress and enforcement for victims.¹⁵⁶ The proposed approach would likely result in fragmented and uneven protection, with the recognition and enforceability of rights varying from one jurisdiction to another. This would not only limit the effectiveness of remedies available for victims (e.g. removal orders), but would also complicate questions of applicable law and jurisdiction.

¹⁴⁹ Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights

¹⁵⁰ Art 13(1)(a) IPRED

¹⁵¹ Art 13(1)(b) IPRED

¹⁵² Case c-367/15 *Stowarzyszenie 'Oławska Telewizja Kablowa' v Stowarzyszenie Filmowców Polskich* *ECLI:EU:C:2017:36*

¹⁵³ Karttunen (n26); Hugenholtz (n26)

¹⁵⁴ Case C-192/04 *Lagardère Active Broadcast* [46] I-7199

¹⁵⁵ Karttunen (n26)

¹⁵⁶ Karttunen (n26); Hugenholtz (n26)

Effective enforcement would remain particularly problematic where deepfakes were to be created, hosted, and disseminated from outside the Netherlands and Denmark. Questions arise as to how national authorities could effectively tackle infringements originating abroad, particularly in light of the interaction with platform take-down obligations under the DSA.¹⁵⁷ The DSA does not provide a uniform definition of “illegal content”; instead illegality is determined by reference to EU and national law and may thus vary across Member States.¹⁵⁸ As clarified by the European Commission, where content is only considered illegal under the law of a particular Member State, it should only be removed in its territory.¹⁵⁹ Applied to the present context, non-consensual deepfakes would only infringe Danish and Dutch national copyright law. Consequently, enforcement actions based on the amended copyright acts may likely only result in the removal within the latter territories. This would be unsatisfactory from a victim’s perspective, for whom the harm largely arises from the widespread and persistent circulation of content online.

In addition to the practical enforcement difficulties outlined, it should be noted that extending copyright or neighbouring rights to individuals depicted in deepfakes appears to offer limited additional protection beyond what provided through personality rights. As discussed above, personality rights already effectively safeguard the privacy and commercial interests of individuals from unauthorised reproductions of their likeness. In particular, the proposed amendments to copyright law do not resolve the conceptual and practical difficulties raised by the application of personality rights to deepfakes. Similarly to what discussed in Section 4 D, application of the new copyright-based rights is likely to be unclear where only partial or minor features of an individual are used and combined with others’ (such that the resulting deepfake no longer depicts an identifiable real individual). Equally, uncertainty remains as to whether protection would also extend to highly stylised or non-photorealistic representations. Ultimately, the proposed amendments fail to significantly extend protection for victims, rather in practice only offering a written codification of longstanding principles of personality rights developed through case law.¹⁶⁰

Finally, granting copyright protection over one’s likeness for digital representations in deepfakes is conceptually inadequate from an incentives-based perspective. The rights contemplated in the Dutch and Danish proposals would open up licensing opportunities for such uses, thereby potentially introducing the risk of exploitative practices (well documented issues e.g. in the music industry).¹⁶¹ Granting rights would only seem to legitimise the harmful behaviour rather than discourage it. This concern follows and builds upon Bartow’s argument that copyright law has historically advanced the commercial interests of those producing and profiting from pornographic imagery, regardless of how it is created.¹⁶² Bartow accordingly suggests denying copyright protection to any material produced by harming individuals’ rights (e.g. child pornography, revenge porn).¹⁶³ Feminist copyright scholars, writing in the context of deepfakes, have taken this critique further by arguing for copyright protection

¹⁵⁷ Karttunen (n26)

¹⁵⁸ Art 3(h) DSA; Laureline Lemoine and Mathias Vermeulen, *The Extraterritorial implications of the DSA*, DSA Observatory (2023) available at : <https://dsa-observatory.eu/2023/11/01/the-extraterritorial-implications-of-the-digital-services-act/>

¹⁵⁹ European Commission, Questions and answers on the DSA (2024) available at: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_2348; Case C-507/17 *Google v CNIL* (2019) ECLI:EU:C:2019:772

¹⁶⁰ Karttunen (n26)

¹⁶¹ See e.g. Davide Arditi, “Record Contracts: Recording Artists, Work, and Exploitation” In: Arditi (eds) *The Palgrave Handbook of Critical Music Industry Studies.*; Jozefien Vanherpe, *Music contracts in the streaming age* (2025)

¹⁶² Ann Bartow, "Copyright Law and Pornography," *91 OR. L. REV. 1* (2012).

¹⁶³ *ibid*

to be contingent on the depicted individual's consent.¹⁶⁴ In the present author's view, denying copyright protection to deepfakes produced without the depicted individual's consent would constitute a more coherent and defensible approach than extending rights to depicted individuals. While denying copyright protection to deepfake creations produced without consent would alone not prevent the creation and circulation of deepfakes, it would reduce creators' ability to profit from such content. This would in turn reduce the economic incentives, which amongst other motives, currently drive deepfake production and dissemination.¹⁶⁵

6. CONCLUSION

The above analysis has argued that proposed amendments to national copyright law fail to enhance protection against deepfakes in any meaningful way. The principal challenge associated with non-consensual deepfakes lies not in the absence of a legal basis for action, but rather in ensuring effective enforcement and redress for victims.¹⁶⁶ EU law and national Member States already provide a broad and overlapping set of protections through diverse areas of law. The suggested amendments to national Danish and Dutch copyright law are thus largely redundant and would likely only introduce additional difficulties in cross-border enforcement.

The key issue that remains to be addressed rather concerns the timely and permanent removal of such forms of content from online platforms. Policy efforts should therefore rather be directed towards strengthening international cooperation and existing enforcement mechanisms to secure prompt and permanent removal of harmful content across jurisdictions. This is crucial given the primary harms of non-consensual deepfakes stem from the psychological and reputational damage caused by their widespread and quick dissemination online.¹⁶⁷ In this regard, the further development and harmonisation of personality rights at EU level would be particularly appropriate, given their current highly fragmented nature across EU member. A more robust and harmonised personality rights regime, coupled with enhanced enforcement mechanisms, would offer a stronger and more coherent approach in combating non-consensual deepfakes and their associated harms.

Deepfakes are far from a new phenomenon; image and video manipulation have always been inherent to these mediums. The parallels between analogue image manipulations and deepfake technology are best exemplified by the numerous documented cases from the late 19th century, when fictitious nude photographs of women were produced by superimposing studio portrait negatives onto images of unclothed models.¹⁶⁸ These images, which could be understood as early precursors of contemporary "deep nudes", demonstrate that the ethical and legal challenges associated with deepfakes are not entirely novel and have already been addressed by existing legal frameworks. The emergence of AI generated deepfakes therefore does not necessitate a radical rethinking of current legal frameworks, but rather a targeted adaptation of existing mechanisms to strengthen enforcement in online environments.

BIBLIOGRAPHY

Legislation

Charter of Fundamental Rights of the European Union

¹⁶⁴ Lake (n36)

¹⁶⁵ Nir Kshetri, "The Economics of Deepfakes," in *Computer*, vol. 56, no. 8 (2023)pp. 89-94

¹⁶⁶ Krack (n7) ; Karttunen (n26)

¹⁶⁷ Ajder et al (n12)

¹⁶⁸ Lake (n36); see e.g. "Le Grange Brown's Pictures", *The New York Times* (26 September 1888)

Universal Declaration of Human Rights

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC

Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

Directive 2004/48/EC of the European Parliament and of the Council of 29 April 2004 on the enforcement of intellectual property rights

Croatian Criminal Code

German Federal Council Drs. 222/24

Kulturudvalget 2024-25 KUU Alm.del - Bilag 232

Danish Neighbouring Rights Act

Dutch Copyright Act

Copyright Law of the United States (Title 17)

Case Law

Case C-145/10 *Eva-Maria Painer v. Standard VerlagsGmbH et al.* ECLI:EU:C:2011:798 (2011)

Case C-393/09 *Bezpečnostní softwarová asociace – Svaz softwarové ochrany v. Ministerstvo kultury* ECLI:EU:C:2010:816 (2010)

Case C-604/10 *Football Dataco Ltd et al. v. Yahoo! UK Ltd et al.* ECLI:EU:C:2012:115 (2012)

Case C-5/08 *Infopaq International A/S v Danske Dagblades Forening* ECLI:EU:C:2009:465 (2009)

C-101/01 *Bodil Lindqvist* ECLI:EU:C:2003:596 (2003)

C-212/13 František Ryneš v Úřad pro ochranu osobních údajů, ECLI:EU:C:2014:2428 (2014)

Case c-367/15 *Stowarzyszenie ‘Oławska Telewizja Kablowa’ v Stowarzyszenie Filmowców Polskich* ECLI:EU:C:2017:36 (2017)

Case C-192/04 *Lagardère Active Broadcast* (2005)

Ugeskrift for Retsvæsen 2015.2936 Ø

Dutch Supreme Court, ECLI:NL:HR:1987:AD0034,

Dutch Supreme Court, *Naturiste 30 October 1987, NJ 1988, 277*

Dutch Supreme Court, *Vondelpark*, 1 July 1998, ECLI:NL:HR:1988:AB7688

Dutch Supreme Court, *Moordenaar G.J. Heijn* 21 January 1994, NJ 1994,473

Dutch Supreme Court, *Nielsen & IPA/Storms Factory; Breekijzer* 2 May 2003, NJ 2004, 80

Dutch Supreme Court, *Cruijff/ Tirion* 14 June 2013, ECLI:NL:HR:2013:CA2788

District Court Amsterdam, *Edgar Davids v Riot Games* 9 August 2017, ECLI:NL:RBAMS:2017:5415

Dutch Supreme Court *Verstappen v PICNIC* 22 April 2022, ECLI:NL:HR:2022:621

Reports:

Ajder, Henry. et al, *The State of Deepfakes: Landscape, Threats, and Impact* (2019);

Article 29 Data Protection Working Party, Opinion 5/2009 on online social networking, 01189/09/EN WP 163, (2009)

Danske Advokater, *Høringsvar over forslag til lov om ændring af lov om ophavsret (Indførelse af en præstationsbeskyttelse og beskyttelse mod digitalt genererede efterligninger mv.)* (20 August 2025)

European Women's Lobby, "*Report on Cyber Violence Against Women*" (September 2024), <https://www.womenlobby.org/NEW-PUBLICATION-Report-on-Cyber-Violence-Against-Women>

Karttunen, Sofia ;*The Danish approach to copyright and deepfakes: A model for the EU?*, EPRS (January 2026)

Law Business Research Report, *Right of Publicity* (2017)

Lemoine, Laureline and Vermeulen, Mathias; *The Extraterritorial implications of the DSA, DSA Observatory* (2023)

Medieradet for Born & Unge, *Høring over udkast til lov om ændring af lov om ophavsret (Indførelse af en præstationsbeskyttelse og beskyttelse mod digitalt genererede efterligninger mv.)* (20 August 2025)

Nicola Lucchi, *Generative AI and Copyright, JURI Committee* (2025)

Pawelec, Maria and Łabuz, Mateusz;; *Non-Consensual Sexualising Deepfakes - Threats and Recommendations for Legal and Societal Action.* (2025) CEE Digital Democracy Watch

The Home Security Heroes, *2023 State Of Deepfakes: Realities, Threats, And Impact* (2024)

van Huijstee, Mariëtte et al, *Tackling Deepfakes in European Policy, European Parliament Report* (2021)

Articles:

Arditi, Davide "Record Contracts: Recording Artists, Work, and Exploitation" In: Arditi (eds) *The Palgrave Handbook of Critical Music Industry Studies.*;

Bartow, Ann "Copyright Law and Pornography," *91 OR. L. REV. 1* (2012).

Block, Martina J; "A Critical Evaluation of Deepfake Regulation through the AI Act in the European Union" *13 Journal of European Consumer and Market Law*, (2024)

Bonadio, Enrico and McDonagh, Luke; ‘Artificial Intelligence as Producer and Consumer of Copyright Works: Evaluating the Consequences of Algorithmic Creativity’ *Intellectual Property Quarterly* (2020)

Buick, Adam ; ‘Copyright and AI Training Data—Transparency to the Rescue?’, *20 J. Intell. Prop. L. & Prac.* (2025)

Diel, Alexander; ‘The harm of deepfakes: a scoping review of deepfakes’ negative effects on human mind and behavior” *AI & Soc* (2025);

Dornis, Tim and Lucchi, Nicola; ‘Generative AI and the Scope of EU Copyright Law: A Doctrinal Analysis in Light of the Referral in *Like Company v. Google*” *IIC* 56, (2025)

Headnotes by Editorial Board, ‘A Lookalike Can Amount to a Portrait under the Copyright Act”, *GRUR* Volume 71(12) (2022)

Hsia, Kian and van den Heuvel, Thijs; ‘Levelling the playing field in eSports – Dutch portrait rights in games”, *Interactive Entertainment Law Review* (2018)

Hugenholtz, Bernt and Quintais, Joao Pedro; ‘Copyright and Artificial Creation: Does EU Copyright Law Protect AI-Assisted Output?”. *IIC* 52 (2021)

Iaia, Vincenzo; ‘To Be, or Not to Be ... Original Under Copyright Law, That Is (One of) the Main Questions Concerning AI-Produced Works”, *71 GRUR* (2022);

Karagianni, Anastasia and Doh, Miriam; “A Feminist Legal Analysis of Non-Consensual Sexualized Deepfakes: Contextualizing Its Impact as AI-Generated Image-Based Violence under EU Law.” *Porn Studies* (2024)

Krack, Noemie ;”Exploring Legal Solutions for Non-Consensual Intimate and Sexually Explicit Deepfakes: Insights from the AI Act, Gender-Based Violence Directive, and Digital Services Act”, *Auteurs en Media* 3/2024 (2025)

Kretschmer, Martin et al, ‘Copyright Law and the Lifecycle of Machine Learning Models”, *IIC* 55 (2024)

Kshetri, Nir "The Economics of Deepfakes," in *Computer*, vol. 56, no. 8 (2023)

Labuz, Mateusz ‘Regulating Deepfakes in the Artificial Intelligence Act, *2 Applied Cybersecurity & Internet Governance* (2023)

Langguth, Johannes et al, ‘Don't Trust Your Eyes: Image Manipulation in the Age of DeepFakes”, *Front Commun* (2021)

Margoni, Thomas and Kretschmer, Martin; ‘A Deeper Look into the EU Text and Data Mining Exceptions: Harmonisation, Data Ownership, and the Future of Technology”, *71 GRUR* (2022)

Meskys, Edvinas et al; ‘Regulating deep fakes: legal and ethical considerations”, *Journal of Intellectual Property Law & Practice*, Volume 15

Moreno, Felipe Romero; “Generative AI and Deepfakes: A Human Rights Approach to Tackling Harmful Content” *International Review of Law, Computers & Technology* (2024);

Qiwei, Li and others, “Reporting Non-Consensual Intimate Media: An Audit Study of Deepfakes” (arXiv,2024)

Rosati, Eleonora; "Copyright as an Obstacle or an Enabler? A European Perspective on Text and Data Mining and its Role in the Development of AI Creativity", *27 Asia Pacific Law Review* (2019)

Rosati, Eleonora; "Infringing AI: Liability for AI-Generated Outputs under International, EU, and UK Copyright Law." *European Journal of Risk Regulation* 16 (2) (2025)

Rothman, Jennifer; "Copyrighting people", *Journal of the Copyright Society* (2024)

Synodinou, Tatiana; "Image Right and Copyright Law in Europe: Divergences and Convergences" *Laws* 3(2) (2014)

van der Sloot, Bart and Wagenveld, Yvette "Deepfakes: regulatory challenges for the synthetic society" *Computer Law & Security Review Vol 46* (2022)

Visser, Dirk; "Deepfakes onder een naburing recht", *Mediaforum* 2024(5) (2024)

Yavuz, Can ;"Criminalisation of the Dissemination of Non-Consensual Sexual Deepfakes in the EU. A Comparative Legal Analysis" (2024) 95 *RIDP*

Chapters:

Brügge-meier, Gert et al. "A Common Core of Personality Protection." In *Personality Rights in European Tort Law*, Brügge-meier et al (eds) (2010)

Brügge-meier, Gert; "Protection of Personality Rights in the Law of Delict/Torts in Europe: Mapping out Paradigms." *Personality Rights in European Tort Law*, Brügge-meier et al (eds) (2010)

Guadamuz, Andres 'Do Androids Dream of Electric Copyright? Comparative Analysis of Originality in Artificial Intelligence Generated Works', in Lee and Liu (eds), *Artificial Intelligence and Intellectual Property* (2021)

Lake, Jessica; "Deepfake and non-consensual pornography: recent iterations of the gendered battle for rights in a photograph" in Jessica C Lai and Kathy Bowrey (eds) *A Research Agenda for Intellectual Property Law and Gender* (2025)

Mezei, Peter; "You Ain't Seen Nothing Yet" - Arguments against the Protectability of AI-generated Outputs by Copyright Law. In: Maurizio Borghi (eds.): *Informational Rights and Informational Wrongs: A Tapestry for Our Times* (2023)

Tyagi, Kalpana; Deepfakes, "Copyright and Personality Rights an Inter-Disciplinary Perspective" In: Mathis, K., Tor, A. (eds) *Law and Economics of the Digital Transformation* (2023).

Ochoa, Tyler; 'Overlaps Between Copyright, Rights of Publicity, and Personality Rights', in Neil Wilkof, Shammad Basheer, and Irene Calboli (eds), *Overlapping Intellectual Property Rights* (2023)

Ondreasova, Eva; "Personality Rights in Different European Legal Systems: Privacy, Dignity, Honour and Reputation", in Oliphant et al (eds) *The Legal Protection of Personality rights: Chinese and European Perspective* (2018)

Riis, Thomas; "The Use of Personal Characteristics in Sports Managers Games" in *Intellectual Property and Sports: Essays in Honour of P. Bernt Hugenholtz*, Martin Senfleben et al (eds)

Zornetta, Alessia and Cofone, Ignacio 'Artificial Intelligence and the Right to Privacy', in Jeroen Temperman, and Alberto Quintavalla (eds), *Artificial Intelligence and Human Rights* (2023)

Books:

Husovec, Martin; *Principles of the Digital Services Act* (2024)

Mitchell, William J; *The Reconfigured Eye: Visual Truth in the Post-Photographic Era* (1994)

Vanherpe, Jozefien *Music contracts in the streaming age* (2025)

Van der sloot, Bart; *Regulating the Synthetic Society Generative AI, Legal Questions and Societal Challenges* (2024)

Blogs:

Abarkan, Hicham; Kamer wil burgers auteursrecht geven op gezicht en stem: David versus Goliath?, Nos Nieuws (15 July 2025)

Hugenholtz, Bernt; ‘‘Deepfake Bills in Denmark and the Netherlands: Right idea, wrong legal framework’’, *Kluwer Copyright Blog* (August 6 2025) available at: <https://legalblogs.wolterskluwer.com/copyright-blog/deepfake-bills-in-denmark-and-the-netherlands-right-idea-wrong-legal-framework/>;

Macdonald, Fiona; ‘‘How a 19th-Century portrait of Abraham Lincoln was later revealed to be a fake’’ BBC (14 March 2024) available at: <https://www.bbc.com/culture/article/20240313-how-a-19th-century-portrait-of-abraham-lincoln-was-later-revealed-to-be-a-fake>

Nieremberg, Amelia; ‘‘Denmark Aims to Use Copyright Law to Protect People From Deepfakes’’, *New York Times* (10 July 2025) available at: <https://www.nytimes.com/2025/07/10/world/europe/denmark-deepfake-copyright-ai-law.html>

US Library of Congress, The Spanish-American War in Motion Pictures available at: <https://www.loc.gov/collections/spanish-american-war-in-motion-pictures/about-this-collection/>

van Trigt, Marjolein; ‘‘Geen auteursrecht op uiterlijk en stem’’, BinnenlandsBestuur, (22 September 2025) available at: <https://www.binnenlandsbestuur.nl/juridisch/geen-auteursrecht-op-uiterlijk-en-stem>

Visser, Dirk; in ‘‘*The Dutch and Danish proposals for legislation on deepfakes*’’, *ItenRecht* (2025) <https://www.itenrecht.nl/artikelen/the-dutch-and-danish-proposals-for-legislation-on-deepfakes>