

University of Hamburg

European Master's Programme in Human Rights and Democratisation
A.Y. 2025/2026

**Reinterpreting the Right to Be Forgotten: A Doctrinal and Feminist Analysis of Article 17 GDPR
in Cases of Non-Consensual Deepfake Pornography.**

Author: Aleksandra Katarzyna Banak
Supervisor: Prof. Dr. Gabriele Margarete Buchholtz

Word Count Declaration: 29 213

We refuse to operate under the assumption that risk and harm associated with data practices can be bounded to mean the same thing for everyone, everywhere, at every time (...) We commit to understanding data as always and variously attached to bodies; we vow to interrogate the biopolitical implications of data with a keen eye to gender, race, sexuality, class, disability, nationality, and other forms of embodied difference (...)

Cifor, M., Garcia, P., Cowan, T.L., Rault, J., Sutherland, T., Chan, A., Rode, J., Hoffmann, A.L., Salehi, N., Nakamura, L. (2019). Feminist Data Manifest-No. Retrieved from: <https://www.manifestno.com/>.

Abstract:

Non-consensual deepfake pornography has become one of the fastest-growing forms of image-based sexual abuse and the people it targets are overwhelmingly women. It causes lasting psychological and reputational harm and strikes directly at human dignity, yet the existing legal response remains fragmentary. Criminal law tends to intervene only once the harm is done and varies considerably between Member States, while the available civil routes such as defamation, copyright, image rights and harassment, each reach only part of the injury. This thesis asks whether the General Data Protection Regulation and specifically the right to be forgotten from Article 17, can offer victims a more effective remedy than these alternatives.

Two doctrinal obstacles stand in the way. The first concerns whether fabricated imagery of an identifiable individual qualifies as personal data and potentially as special-category data under Article 9. Drawing on the case law of the Court of Justice, the thesis argues that the question should turn on the effect of the processing on the data subject rather than on the authenticity of the image. The second obstacle lies in the balancing exercise under Article 17(3)(a), which presumptively treats synthetic intimate imagery as protected expression. Through a feminist reading of that framework, the thesis shows that the presumption is far from neutral and works to the systematic disadvantage of victims.

Combining doctrinal analysis with feminist legal theory and grounding its argument in Articles 1, 3, 7 and 8 of the Charter of Fundamental Rights together with the substantive-equality guarantee in Article 23, the thesis proposes a constitutionally consistent reinterpretation of Article 17. It acknowledges the limits of this approach and positions the right to erasure as one component of an integrated European response, working alongside the AI Act, the Digital Services Act and Member State criminal law.

ABSTRACT	3
INTRODUCTION	6
Chapter I Non-Consensual Deepfake Pornography: The Phenomenon and Its Harms	8
1.1 Defining Deepfakes: Technology, Process and Terminology	8
1.2 The landscape and gendered patterns of victimisation of non-consensual deepfake pornography	10
1.3 The nature of the harm	14
1.4 The Theoretical Framework: Feminist Theories of Digital Embodiment.....	20
1.5 The Legal Gap: Why Existing Frameworks Fall Short.....	25
Chapter II Synthetic Identity and the Limits of Personal Data	29
2.1 The concept of personal data under article 4(1) GDPR	29
2.2 Court of Justice of the European Union’s case law on personal data and its implications	32
2.3 The challenge of deepfakes: hybrid form of data	35
2.4 The inadequacy of traditional identifiability framework	38
Chapter III The Right to Erasure: Scope and Limitations	42
3.1 Development, Conditions Triggering and Obligations of Controllers under article 17 GDPR	42
3.2 Delisting Versus Deletion: A Critical Distinction	44
3.3 Procedural and Practical Limitations	46
3.4 The Remedial Value of Legal Recognition	49
Chapter IV When Expression Trumps Dignity: The Structural Bias of the Exceptions Framework	52
4.1 The Exceptions Under Article 17(3): An Overview	52
4.2 Freedom of Expression and the Balancing Framework	53
4.3 The Structural Bias Problem	56
4.4 Public Interest Across the Framework.....	59
Chapter V Feminist Reinterpretation of Article 17: Dignity, Consent, and Digital Integrity	61

5.1 The Charter as the Interpretive Foundation	61
5.2 Reinterpreting "Personal Data"	64
5.3 Reinterpreting "Erasure"	67
5.4 The Limits of Reinterpretation	69
5.5 Practical Implications and Improvements Stemming from Feminist Reinterpretation	71
CONCLUSION	75
BIBLIOGRAPHY	77

INTRODUCTION

Non-consensual deepfake pornography is one of the most rapidly expanding forms of gendered harm and sexual abuse. The technology that generates it has become widely accessible, the platforms that host it operate with little effective oversight and the volume of synthetic intimate imagery circulating online has grown by over 500% between 2019 and 2023.¹ About 97% of deepfake videos available online are pornographic and 96% of people depicted in them are women.² These statistics describe the structure of a harm that the existing legal landscape has, so far, failed to address.

Each of the obvious alternatives fails in a different way. Criminal law is fragmented across Member States and, in any event, arrives only once the harm is done; defamation law, built around false statements of fact, struggles with fabrications that are openly acknowledged as fabrications; copyright protects whoever created the synthetic image not the person depicted in it; image rights and harassment law reach only fragments of the injury. Within this landscape, the General Data Protection Regulation emerges as the most promising existing legal instrument available to victims. It applies to the processing of personal data, imposes obligations on controllers and provides through Article 17 a right to erasure that no other framework currently matches in reach or directness.³ That potential is real, but the framework as currently interpreted has not been made to deliver on it for victims of non-consensual deepfake pornography.

The question this thesis addresses is whether that failure is structural, and if so, whether it can be addressed through reinterpretation of existing provisions rather than through new legislation. The argument advanced is that the GDPR's right to erasure, properly read in light of the Charter of Fundamental Rights and through a feminist legal theory lens, can be made to recognise and respond to the harm in ways that the case law has not yet developed. The reinterpretation rests on three constitutional pillars: the dignity and integrity provisions of Articles 1 and 3 of the Charter, the data protection guarantees of Articles 7 and 8, and the substantive equality requirement of Article 23.⁴ Together these provisions require an interpretation of "personal data" under Article 4(1) and of "erasure" under Article 17 that goes beyond what the current case law has developed. This reading does not reproduce the gendered pattern of weaker protection that the existing framework produces.

¹ Henry Ajder and others, *The State of Deepfakes: Landscape, Threats, and Impact* (Deeprace 2019); Security Hero, 2023 *State of Deepfakes Report* (2023).

² *ibid*

³ GDPR, art. 17.

⁴ Charter of Fundamental Rights of the European Union [2012] OJ C326/391, arts 1, 3, 7, 8, 23.

The methodology used in developing this argument combines doctrinal analysis with feminist legal theory. Doctrinal analysis does the first job: working out what the GDPR's provisions currently mean and how the CJEU has read them. The feminist half of the argument is different in kind, it asks what those readings assume, what they leave out and whose harms, as a result, go unregistered. The two approaches are not in competition. Feminist theory here is an analytical lens that informs doctrinal interpretation, with its basis in the Charter's substantive equality requirement which makes the feminist work doctrinally available. MacKinnon's analysis of how law reproduces male perspective as objectivity provides the structural diagnosis,⁵ Citron's framework of sexual privacy bridges that diagnosis to the question of legal remedy⁶ and Öhman's concept of representational injury identifies the moment at which the harm of non-consensual synthetic intimate imagery begins.⁷

The argument develops across five chapters. Chapter 1 establishes the nature and scale of non-consensual deepfake pornography, the gendered pattern of victimisation that runs through it and the feminist theoretical framework through which it must be analysed. Chapter 2 examines the concept of personal data under Article 4(1), arguing that the traditional identifiability framework offers stronger protection to publicly recognisable victims than to private individuals and that this asymmetry tracks the gendered structure of the harm itself. Chapter 3 turns to the right to erasure under Article 17, examining its scope, the practical distinction between delisting and deletion and the procedural and remedial limitations that constrain it in practice. Chapter 4 analyses the exceptions to the right under Article 17(3), showing that the balancing framework the CJEU has developed presumes expressive value in ways that systematically disadvantage victims of non-consensual deepfake pornography. Chapter 5 develops the feminist reinterpretation of the right that the preceding chapters establish as necessary.

The reinterpretation cannot turn the GDPR into a comprehensive remedy and it does not claim to. Erasure delivers removal rather than redress and the regulation reaches controllers rather than the creators of the content. Many platforms hosting deepfake material fall outside its territorial scope and supervisory authorities are constrained by limited resources and uneven institutional cultures. What it can do is make the GDPR meaningfully available within its proper scope, as one component of an integrated EU response that also includes the AI Act, the Digital Services Act and Member State criminal law, each addressing what the others leave untouched.

⁵ Catharine A MacKinnon, *Toward a Feminist Theory of the State* (Harvard University Press 1989) ch 13.

⁶ Danielle Keats Citron, 'Sexual Privacy' (2019) 128 *Yale Law Journal* 1870.

⁷ Carl Öhman, 'Introducing the Pervert's Dilemma: A Contribution to the Critique of Deepfake Pornography' (2020) 22 *Ethics and Information Technology* 133.

Chapter I Non-Consensual Deepfake Pornography: The Phenomenon and Its Harms

1.1 Defining Deepfakes: Technology, Process and Terminology

Technological advancement has both changed and expanded the range of ways in which sexual violence can be committed. Nowadays sexual harm can be inflicted on a person outside of the physical world. With the rapidly growing use of Artificial Intelligence (AI) new manifestations of abuse emerged.⁸ One of them is the non-consensual creation and/or distribution of private sexual images created with the use of artificial intelligence tools, the so-called deepfake pornography. A phenomenon that can be defined as a part of broader issue, the “image-based sexual abuse”.⁹ As this is a rapidly growing “trend”, numerous terms have emerged in the literature on that subject. For the purposes of this paper, the terms “synthetic intimate imagery” and “non-consensual deepfake pornography” are used synonymously and should be understood in the same way. They are defined as “non-consensual creation and/or distribution of private sexual images created with the use of artificial intelligence tools”.¹⁰ These two expressions best convey the essence of this issue by both placing strong emphasis on the harm that can result and reflecting the experiences of survivors.¹¹ The other important element of the definition is locating it within the scope of interest of the legislator and law in general. By using word “non-consensual” we are moving into an area that should and can be subject to legal regulations.¹²

To fully grasp the seriousness of this issue, it is important to understand how deepfakes are created and what they are. The technology utilizes machine learning algorithms to superimpose faces and voices onto video and audio recordings of real people and enables the creation of realistic digital imitations from scratch.¹³ The result is a hyper realistic-looking video or audio clip that gives the impression that someone said or did something.¹⁴ Although deepfakes can be created with the consent of the people who appear in them, they are more often created without that consent. The practice of tampering with photos or videos is by no means new or surprising. Tools like Photoshop have been widely available for many years, but until now, it has been easy to detect images that have been altered using such tools. The emergence of generative technology based on machine learning has changed that. It has allowed for the

⁸ Clare McGlynn and Erika Rackley, 'Image-Based Sexual Abuse' (2017) 37 Oxford Journal of Legal Studies 534, 1.

⁹ *ibid*

¹⁰ *ibid* 3

¹¹ *ibid*

¹² Nicola Henry and Anastasia Powell, 'Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law' (2016) 25 Social & Legal Studies 397-418.

¹³ Robert Chesney and Danielle Keats Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753.

¹⁴ *ibid*

creation of entirely fabricated images, which are far more realistic and harder to debunk than ever before.¹⁵

Deepfake images are produced using a type of artificial intelligence called deep neural networks.¹⁶ The technology works by processing large datasets of real images through layered computational systems capable of generating synthetic output that is increasingly indistinguishable from authentic footage.¹⁷ Once a network has absorbed enough information from its training data it can begin generating entirely new ones. By drawing on everything it has learned about how real images look, the network can produce pictures from scratch that are nearly indistinguishable from genuine photographs. The same principle is being extended to video, though this remains more technically demanding. Current models struggle to handle it perfectly, however soon they will be as accurate and as deceivable as with the creation of still images.¹⁸ By 2017, researchers had demonstrated the technology's capacity to fabricate convincing video of public figures speaking words they had never said.¹⁹

The development of machine learning based on neural networks alone represents a huge leap forward in the creation of synthetic images. Nevertheless, this technology has advanced even further thanks to the development of so-called generative adversarial networks (GANs).²⁰ The development of GANs, in which two neural networks operate in a continuous feedback loop to produce and refine synthetic content, accelerated this trajectory significantly. The results far exceed what any human reviewer could achieve in speed, scale and subtlety and the technology has since been made available to non-specialist users through consumer-facing applications.²¹

Many user-friendly tools have already been created. One of the first of such was an app called Fake App. Its purpose was described by its creators as “a desktop app for creating photorealistic

¹⁵ *ibid* 1759

¹⁶ Will Knight, 'Real or Fake? AI is Making it Very Hard to Know' (MIT Technology Review, 1 May 2017) <https://www.technologyreview.com/s/604270/real-or-fake-ai-is-making-it-very-hard-to-know> accessed 10 April 2026.

¹⁷ *ibid*

¹⁸ *ibid*

¹⁹ Supasorn Suwajanakorn and others, “Synthesizing Obama: Learning Lip Sync from Audio” (2017) 36 ACM Transactions on Graphics, art. 95, http://grail.cs.washington.edu/projects/AudioToObama/siggraph17_obama.pdf; James Vincent, New AI Research Makes It Easier to Create Fake Footage of Someone Speaking, (the verge, 12 July 2017), <https://www.theverge.com/2017/7/12/15957844/ai-fake-video-audio-speech-obama>, both cited in Chesney and Danielle K Citron, (n 13), 1760.

²⁰ Ian J Goodfellow and others, 'Generative Adversarial Nets' (Neural Information Processing Systems Conference Paper, 10 June 2014) <https://arxiv.org/abs/1406.2661> accessed 10 April 2026.

²¹ Tero Karras and others, 'Progressive Growing of GANs for Improved Quality, Stability, and Variation' (ICLR Conference Paper, April 2018) http://research.nvidia.com/sites/default/files/pubs/2017-10_Progressive-Growing-of/karras2018iclr-paper.pdf accessed 10 April 2026.

faceswaps videos made with deep learning”²². Nowadays one of the most popular tools used to create those fake images, is a tool called DeepSwap.²³ It is described as user-friendly and having an easy online accessibility.²⁴ It is possible to install the app both on mobile devices and laptops. Main features of the app are the speed in which it can create a deepfake image and the closeness in which the generated images mimic the reality.²⁵ The terms of service of DeepSwap strictly prohibit the creation and distribution of pornographic deepfakes, but it is not a problem since there are plenty of services that advertise themselves as “allowing to turn any person into a 'porn star' by uploading their photo onto the website, which uses deepfake technology to swap the person's face into an adult”.²⁶

Estimates suggest that more than 95% of deepfake videos on the Internet in 2019 were pornographic and 96% of them depict women.²⁷ These figures reflect a clear and deliberate pattern of gendered misuse, one that reveals deepfake technology as having been adopted primarily as an instrument of sexual exploitation

1.2 The landscape and gendered patterns of victimisation of non-consensual deepfake pornography

The scale, accessibility and gendered character of this form of abuse are not background facts. They are central to understanding why existing legal frameworks have proven inadequate and why the feminist reinterpretation advanced in this thesis is necessary. What the evidence reveals is a large-scale, rapidly expanding industry of harm, that has developed in near-total absence of effective legal constraint. Content creation using artificial intelligence, which was once a complex and resource-intensive process, is now fully accessible to a wide range of users, enabling creators of all skill levels to use advanced AI tools with unprecedented ease.²⁸

²² FAKEAPP, <https://www.fakeapp.org> accessed 10 April 2026.

²³ Sami Alanazi and Seemal Asif, 'Exploring Deepfake Technology: Creation, Consequences and Countermeasures' (2024) 6 Human-Intelligent Systems Integration 49), 51.

²⁴ *ibid*

²⁵ *ibid*

²⁶ Rangita De Silva De Alwis and Paul Carey, 'A Rapidly Shifting Landscape: Why Digitized Violence is the Newest Category of Gender-Based Violence' (2023) Public Law and Legal Theory Research Paper Series, Research Paper No 23, 8.

²⁷ Meredith Somers, 'Deepfakes, explained' (MIT Sloan Management Review, 21 July 2020) <https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained> accessed 10 April 2026.

²⁸ Francesco Cavalli and others, The State of Deepfakes 2024 (Sensity AI 2024) <https://5865987.fs1.hubspotusercontent-na1.net/hubfs/5865987/SODF%202024.pdf> accessed 11 April 2026.

The technical infrastructure underpinning deepfake creation had, by 2024, become extensively commodified. Sensity AI documented 2,298 publicly accessible tools for face swap, lip sync, face reenactment and AI-avatar generation, 10,206 tools for AI image generation, and 1,018 tools for voice generation and cloning. These figures demonstrate that non-consensual deepfake pornography is a phenomenon of significant and rapidly expanding scale. The number of deepfake videos is growing at a rate of 900% per year- from 500,000 videos available online in 2023 to 8 million in 2025, 96% of these being pornographic.²⁹ The scale of this phenomenon poses a challenge to current detection capabilities, underscoring the need for continuous development of detection technologies, digital literacy education and, above all, improvements to the legal framework for protecting victims. The misuse of deepfake technology remains one of the most widespread threats in the digital environment.

Nonconsensual deepfake pornography does not exist in a legal or conceptual void. It is part of a broader spectrum of image based sexual abuse. This phenomenon includes the sharing of real intimate photos without the victim's consent, commonly referred to as "revenge porn," as well as upskirt photography, sextortion and the recording of sexual acts without the victim's consent.³⁰ That said, while it shares certain features with these forms of abuse, it differs from them in ways that are significant from a legal and conceptual point of view. The most significant difference stems from the absence of any original sexual imagery. In the case of traditional non-consensual pornography, there is genuine intimate imagery which was either created with consent and then shared without consent or recorded without the victim's knowledge. In other words, the victim participated in the depicted situation at some point. Deepfake pornography does not require such an original image. The perpetrator needs only a publicly available photo. This could be a profile picture from a social media platform, a professional portrait or a photo taken at a public event. Having any online presence is sufficient to generate a synthetic representation of that person of an unambiguously sexual nature.³¹ This has far-reaching implications for the scope of potential victimization. While traditional image-based exploitation assumes a certain degree of prior closeness or intimacy between the perpetrator and the victim, deepfake pornography makes virtually anyone online a potential target. This represents a qualitative shift in the nature of the threat, transforming harm that was once tied to intimate relationships into harm that can be inflicted by a

²⁹ Mohammed Khalili, Deepfake Statistics 2025: AI Fraud Data & Trends, 8 September, 2025, <https://deepstrike.io/blog/deepfake-statistics-2025> accessed 11 April 2026.

³⁰ Clare McGlynn, Erika Rackley and Ruth Houghton, 'Beyond "Revenge Porn": The Continuum of Image-Based Sexual Abuse' (2017) 25 Feminist Legal Studies, 25.

³¹ Francesco Cavalli and others, The State of Deepfakes 2024 (Sensity AI 2024) <https://5865987.fs1.hubspotusercontent-na1.net/hubfs/5865987/SODF%202024.pdf> accessed 11 April 2026

stranger. It even eliminates the need for prior contact with the victim.³² In cases of revenge porn, the victim participated in the creation of the original image and the voluntary nature of its subsequent distribution is independent of that fact. In contrast, the victim of a deepfake did not participate in the depicted act at all. Consequently, the sexual behaviour depicted is entirely fabricated. This distinction carries legal consequences. It reveals a gap in the legal framework, which was constructed around the concept of a legitimate image whose creation and distribution can be traced, proven, and subject to legal proceedings. Deepfakes significantly complicate this evidentiary framework, as the perpetrator can claim that the image is not real. However, and this is crucial, the harm suffered by the victim does not depend on the authenticity of the image.³³ The psychological, reputational and dignitary harm caused by the circulation of a convincing synthetic sexual image is functionally identical to that caused by a real one. In some respects, it may be even more difficult to remedy, precisely because the fabricated nature of the content can be used to trivialise or dismiss the victim's experience.³⁴ Deepfake-based pornography is distinguished by its potential for mass production and automation. Traditional image-based abuse, while serious, is typically limited by the existence of a finite number of real photos. Deepfake technology allows for the rapid and scalable generation of synthetic content, meaning that a single victim can be exposed to a virtually unlimited amount of fabricated material. Combined with the ease of online distribution and the permanence of digital content once shared, this creates a situation where the harm has potentially inexhaustible reach.³⁵

Finally, deepfake pornography introduces a structural ambiguity that is absent in other forms of image exploitation. When a genuine intimate photo is shared without consent, there is no doubt as to whether the depicted behaviour took place. The dispute concerns solely consent to distribution. In the case of deepfakes, the perpetrator retains the capacity to deny the seriousness of the harm by pointing to the fabricated nature of the content, which has the potential to undermine the victim's credibility and complicate both criminal proceedings and civil claims. This dynamic, in which the artificial nature of the image simultaneously enables harm to be inflicted and serves as a defence against liability, is a structural feature of deepfake-related abuses that existing legal frameworks do not yet sufficiently address.³⁶

³² Danielle Keats Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* (W W Norton 2022).

³³ Clare McGlynn and Erika Rackley, 'Image-Based Sexual Abuse' (2017) 37 *Oxford Journal of Legal Studies* 534, 10.

³⁴ *ibid*

³⁵ Henry Ajder and others, *The State of Deepfakes: Landscape, Threats, and Impact* (Deeptrace 2019) https://regmedia.co.uk/2019/10/08/deepfake_report.pdf accessed 11 April 2026.

³⁶ Robert Chesney and Danielle Keats Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 *California Law Review* 1753.

Another aspect of non-consensual deepfake pornography that only serves to underscore how dangerous and harmful this phenomenon is concerns the gendered nature of the harm. Deepfake pornography is a phenomenon that overwhelmingly targets and harms women.³⁷ 96% of deepfake videos posted on pornographic websites feature women.³⁸ In contrast, deepfake videos posted on YouTube feature mostly men.³⁹ The most commonly depicted women are actresses, musicians and politicians.⁴⁰ While public figures represent the most visible targets, private individuals are increasingly subjected to deepfake pornography, often by acquaintances, former partners or strangers who have accessed photographs through social media. This expansion of the victim pool beyond the public sphere fundamentally undermines any suggestion that the harm is confined to those who have voluntarily entered public life.

Gendered harm here doesn't operate uniformly, either. The Deepttrace report identified that a significant proportion of targeted women came from non-Western backgrounds, suggesting that race and ethnicity compound vulnerability in ways that a purely gender-based analysis risks obscuring.⁴¹ A feminist framework adequate to the phenomenon must therefore be intersectional in character, attentive to the ways in which gender-based harm is shaped and intensified by race, ethnicity and other axes of structural disadvantage.

“Deepfake technology is being weaponized against women by inserting their faces into porn. It is terrifying, embarrassing, demeaning, and silencing. Deepfake sex videos say to individuals that their bodies are not their own and can make it difficult to stay online, get or keep a job, and feel safe.”⁴² The consequences of deepfake pornography extend beyond the individual victim. The chilling effect produced by the knowledge that any woman with an online presence may be targeted, suppresses women's participation in public discourse, professional environments and political life. In this sense, the harm is democratic. It functions as a structural mechanism of exclusion that disproportionately diminishes women's voices in the spaces where they are already underrepresented.

³⁷ Henry Ajder and others, *The State of Deepfakes: Landscape, Threats, and Impact* (Deepttrace 2019) https://regmedia.co.uk/2019/10/08/deepfake_report.pdf accessed 11 April 2026.

³⁸ *ibid*

³⁹ *ibid*

⁴⁰ *ibid*

⁴¹ Henry Ajder and others, *The State of Deepfakes: Landscape, Threats, and Impact* (Deepttrace 2019) https://regmedia.co.uk/2019/10/08/deepfake_report.pdf accessed 11 April 2026.

⁴² *Ibid*. Citing Danielle Citron, Professor of Law, Boston University, private correspondence with the author of the report, August 16 2019.

In the report of the United Nations Special Rapporteur on violence against women its causes and consequences, Dubravka Šimonović, puts AI facilitated violations as a part of all forms of online violence against women and girls.⁴³ Notably, the Rapporteur refrains from establishing a closed catalogue of forms of abuse, reflecting the rapidly evolving nature of the phenomenon. She states that gendered character of online violence is not incidental but structural. Women and girls are disproportionately subjected to its most severe manifestations, a pattern that reflects and reinforces wider inequalities rooted in patriarchal social organisation and systemic discrimination.⁴⁴ Victims of online violence frequently encounter a compounding harm in the form of gender stereotyping that delegitimises their experiences, conduct that international human rights frameworks expressly prohibit. Far from constituting a neutral public sphere, the internet has become a site of sustained gender-based violence, encompassing non-consensual pornography, privacy breaches and the proliferation of content that normalises the subordination of women and girls.⁴⁵

That the law has failed to adequately respond to a harm so overwhelmingly directed at women is not, from a feminist perspective, a coincidence. It reflects a broader pattern in which legal systems have historically been slow to recognise and remedy harms that fall predominantly on women, particularly where those harms occur in spaces that have been inadequately regulated. The inadequacy of existing frameworks, including the GDPR's right to erasure, must therefore be understood as a gendered gap, demanding a correspondingly feminist response.

1.3 The nature of the harm

The gendered dimension of non-consensual deepfake pornography is reflected, amongst other things, in the nature of the harm itself. Women are disproportionately represented among victims of sexual privacy violations, while men constitute the overwhelming majority of perpetrators- an asymmetry documented across multiple jurisdictions.⁴⁶ According to Australia's eSafety Commissioner, women are

⁴³ UN Special Rapporteur on Violence Against Women, Online Violence Against Women and Girls: A Form of Gender-Based Discrimination (A/HRC/38/47, 2018).

⁴⁴ *ibid*

⁴⁵ *ibid*

⁴⁶ Danielle Keats Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* (W W Norton 2022) 39.

twice as likely as men to be subjected to this form of abuse.⁴⁷ Therefore understanding the precise character of the harm inflicted is a legal and theoretical necessity. The harm suffered by victims of non-consensual deepfake pornography is multi-dimensional in nature and can be analysed across different categories.

Non-consensual deepfake pornography shatters victims' self-esteem. Being forced into such an explicit scenario makes them feel as though they have lost control over their bodies, minds and intimate lives. It revokes their sexual autonomy in the most fundamental sense by stripping them of agency over their own image and identity without warning and without recourse. In the survivors' statements documented by Citron, women affected by this phenomenon describe feeling constantly worried that their friends and colleagues would see them only as a nude body, reduced to their most intimate and fabricated representation.⁴⁸ They describe feeling trapped in a permanent state of what one survivor termed "virtual rape"- a condition of violation that does not end when the screen is turned off.⁴⁹

The feeling of fear and constant vigilance is debilitating. It can make victims afraid to take the very actions that led to the violation in the first place. In the case of deepfake pornography, that action is simply having an online presence, something that is nearly impossible to avoid in the contemporary world. Unlike other forms of image-based abuse where a victim might, however unfairly, be advised to avoid sending intimate images, the victim of deepfake pornography has done nothing more than exist digitally. There is no behaviour to modify, no precaution that would have prevented the harm and the experience cannot be escaped.

The psychological damage is severe and can last for years. According to researchers, most victims experience physical, emotional and psychological trauma that can lead to chronic conditions such as depression or post-traumatic stress disorder.⁵⁰ As many as 93% of victims of non-consensual deepfake pornography reported experiencing severe emotional distress.⁵¹ Victims stop speaking out and withdraw from social life. They delete their social media accounts which for some are the only means of maintaining contact with friends and family. But the consequences can be even more serious, ranging

⁴⁷ *ibid*

⁴⁸ *ibid* 41

⁴⁹ *ibid*

⁵⁰ Nicola Henry and Anastasia Powell, 'Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law' (2016) 25 *Social & Legal Studies* 397.

⁵¹ Cyber Civil Rights Initiative, *End Revenge Porn: A Survey of Victims* (CCRI 2014) <https://cybercivilrights.org> accessed 12 April 2026.

from exclusion from communities they once considered safe spaces and in the most tragic cases, ending in suicide.⁵² All because a woman dared to post an ordinary, non-sexual photograph of herself online.

The harm is further compounded by the intersection of gender with race and identity. When a white woman's fabricated nude image appears in search results, she risks being perceived as, in Citron's words, a "damaged slut."⁵³ For women of colour, the injury is layered with an additional dimension of racial stereotype. They are more likely to be regarded as undeserving of privacy. Their victimisation attributed to a hypersexualisation that is itself a product of structural racism rather than anything they have done. For trans and non-binary women, the exposure of their bodies in fabricated pornographic content carries the additional burden of transphobic stigma, their images rendered as objects of disgust or spectacle. In each case, the harm is structural, shaped by the same systems of inequality that deepfake pornography both reflects and reinforces. The psychological devastation described above does not exist in isolation. It spills inevitably into every other dimension of a victim's life: her professional standing and, crucially, her place in the world beyond the screen.

Reputational and professional harm almost invariably follow and they carry severe economic consequences. Employers decline to interview, hire or retain individuals whose names return explicit results in online searches.⁵⁴ Women lose their jobs and find themselves unable to obtain new ones. Depending on the nature of the content depicted, victims may even face legal scrutiny themselves, an inversion of justice so complete as to be almost incomprehensible. The legal framework's failure to prevent this inversion, holding the victim of fabrication to account for content she never created and never consented to, reflects the same structural blindness that the following chapters identify in the GDPR's approach to deepfake harm. Yet even reputational and professional destruction does not capture the full depth of what is taken from a victim of non-consensual deepfake pornography. Beneath the lost job and the broken career lies something more fundamental, a violation of the victim's very standing as a human being.

"Women are presented as sexual objects for domination, violation, exploitation, possession, or use..."⁵⁵, they are "dehumanized as sexual objects, things or commodities."⁵⁶. This is the essence of

⁵² Danielle Keats Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* (W W Norton 2022) 42.

⁵³ *ibid*

⁵⁴ *ibid* 44

⁵⁵ Catharine A MacKinnon, *Feminism Unmodified: Discourses on Life and Law* (Harvard University Press 1987) 262.

⁵⁶ *ibid* 174.

dignitary harm as it manifests in non-consensual deepfake pornography. It is a harm that strikes at something more fundamental than reputation or emotional wellbeing. It strikes at the very recognition of a person as a person. To understand why, it is worth turning first to Immanuel Kant. For Kant, every human being possesses an inherent dignity that cannot be taken away. It does not depend on what a person looks like, what they do or how others perceive them. It is absolute and it comes with a demand, that a persons must always be treated as ends in themselves, never just as means to someone else's ends.⁵⁷ To use a person as a tool for your own gratification, amusement or malice is a fundamental denial of their humanity. This is precisely what happens when someone creates non-consensual deepfake pornography. The victim is not consulted. She is not considered. She is simply used as material for content she never agreed to and would never have permitted.

Martha Nussbaum took this idea further by identifying seven specific features of objectification, each of which represents a distinct way in which a person's dignity can be violated.⁵⁸ The first is instrumentality- the treatment of a person as a tool for another's purposes. The second is denial of autonomy- the refusal to recognise the person's capacity for self-determination and independent choice. The third is inertness- the treatment of the person as passive, as something that things happen to rather than someone who acts. The fourth is fungibility- the treatment of the person as interchangeable with any other of the same type, denying their individuality and uniqueness. The fifth is violability- the treatment of the person as lacking in boundary integrity, as something that can be broken into or invaded without moral consequence. The sixth is ownership- the treatment of the person as property, as something that can be possessed, used and disposed of. The seventh is denial of subjectivity- the treatment of the person as something whose inner experiences, feelings and perspective are irrelevant.⁵⁹ What makes Nussbaum's framework so analytically powerful in the context of non-consensual deepfake pornography is that all seven features can be applied. The perpetrator uses the victim's image as a tool for their own gratification or malicious purpose, satisfying the criterion of instrumentality. They override the victim's explicit non-consent, denying her autonomy in the most direct sense imaginable. They render her passive and entirely unable to control her own representation, reducing her to a state of inertness. They treat her as interchangeable with any other woman whose photograph is publicly accessible online, treating her as fungible. They penetrate the most intimate boundary of bodily representation without consent, committing the precise violation that Nussbaum's concept of violability describes. They treat her image

⁵⁷ Immanuel Kant, *Groundwork of the Metaphysics of Morals* (Mary Gregor tr, Cambridge University Press 1998) 38.

⁵⁸ Martha C Nussbaum, 'Objectification' (1995) 24 *Philosophy and Public Affairs* 249, 257.

⁵⁹ *ibid*

as something they are entitled to possess, manipulate and distribute, asserting a form of ownership over her identity that she never granted. They proceed as though her feelings, her humanity and the consequences for her life are entirely irrelevant- denial of subjectivity.

The fact that all seven features apply so completely and so precisely shows that non-consensual deepfake pornography is not some new and unrecognisable harm that the law has no tools to address. Not every feature applies with equal force in every case and pressing all seven onto every instance risks flattening real variation between cases but the fit here is close enough that the framework does real analytical work. Feminist legal theory has already developed the language to describe exactly what is happening to these women. What is missing is the legal framework willing to take it seriously. Dignitary harm of this kind, total, systematic and rooted in the complete denial of a woman's personhood, cannot be addressed by legal frameworks built only around reputational damage or the distribution of real images. It demands a legal response that recognises what is being violated, not just a woman's good name, but her fundamental standing as a human being with the right to control her own identity, her own body and her own story. Closely connected to dignitary harm, though distinct from it, is a form of injury that can be seen at an even earlier stage, before distribution, before discovery and before the victim has any knowledge that she has been violated at all.

Representational injury is a concept that comes from Carls Öhman's *The Perverts Dilemma*. A deepfake image that has been created but never shared still causes harm to the person depicted, because their identity and likeness have been used without consent to create a sexual narrative that they themselves never consented to.⁶⁰ This poses a challenge to models based on the assumption that it is dissemination and visibility that constitute the threshold at which harm occurs. A key element of this argument is the concept of control over one's own narrative, a person's right to decide how their sexual identity is portrayed to the world.⁶¹ Deepfake pornography violates this right the moment it is manufactured, not just when it is distributed. Öhman further argues that our images constitute an integral part of our identity. Consequently, fabricating a sexual image of a person means creating a false version of who they are and introducing it into the world without their knowledge or consent. The harms examined so far are suffered primarily by those who have already been victimised. The silencing effect,

⁶⁰ Carl Öhman, 'Introducing the Pervert's Dilemma: A Contribution to the Critique of Deepfake Pornography' (2020) 22 *Ethics and Information Technology*, 134.

⁶¹ *ibid*

however, extends the reach of non-consensual deepfake pornography beyond individual victims to society as a whole.

A woman considers entering public life: politics, journalism, academia, any field that brings visibility. She knows that visibility makes her a target. She knows that having a public profile, a professional photograph, a social media presence, is enough for someone to fabricate explicit content featuring her face. And so, she does not enter. She stays silent before she has even had the chance to speak. This is the silencing effect and it can affect every woman who watches how the ones that spoke out are victimised. Since more female politicians are becoming victims of this phenomenon, more and more women are becoming afraid of being inserted into pornographic content without their consent. The consequence is that fewer women are choosing to enter politics precisely because doing so would make them more likely to become targets. When victims of those violations withdraw from both online and offline activities, we are left with less diverse and less rich public conversations.⁶² The spaces where decisions are made parliaments, newsrooms, boardrooms, all become less representative not because women are less capable or less willing, but because the cost of visibility has been made unbearably high. There are already concrete examples of this dynamic playing out. Female politicians have stepped down from their positions after deepfake pornographic content featuring them was created and distributed.⁶³ The case of Katie Hill is among the most documented- a sitting United States Congresswoman who resigned from office following the non-consensual distribution of intimate images, a case that illustrates with painful clarity how the weaponisation of a woman's body, real or fabricated, can be used to remove her from public life entirely.

The silencing effect creates a democratic harm. It distorts the composition of public life, systematically removing and deterring women from the spaces where they have historically been underrepresented to begin with. A legal framework that fails to address this harm is not neutral, it is complicit. The inadequacy of existing frameworks, including the right to erasure under Article 17 GDPR, must be understood in this light.

⁶² Danielle Keats Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* (W W Norton 2022) 45.

⁶³ See Katie Hill, 'When a Politician's Nude Photos Are Leaked' (BBC, 2019) <https://www.bbc.com/audio/play/w3cszc27> accessed 11 April 2026; see also Danielle Keats Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* (W W Norton 2022) 46.

1.4 The Theoretical Framework: Feminist Theories of Digital Embodiment

It is crucial to analyse and regulate the issue of non-consensual deepfake pornography, through the lens of feminist legal theory. It is because it is not a gender-neutral issue, nor it is a technical problem and a data management challenge. It is a gendered harm caused overwhelmingly by men, directed mostly on women and rooted in structures of patriarchal power that long predate the internet. It cannot be analysed simply through a technological lens. If we don't go beyond establishing whether a particular image meets the identifiability threshold under art. 4(1) GDPR, we are erasing women's experiences from the process, we are essentially silencing the victims.

Feminist legal theory is the necessary analytical framework. It utilizes questions that other frameworks don't such as who is harmed and who is doing the harm. It also asks a harder question: what structural conditions make that harm possible and what makes it persist. It refuses to treat law as a neutral instrument operating above the social world. Instead, it asks whose interests law reflects, whose experiences it renders invisible and whose harms it consistently fails to remedy. Law is not simply a tool that can be picked up and used for feminist purposes. It is a site of power, one that historically has been shaped by and in the interest of male dominance.⁶⁴ To engage with law from a feminist perspective is therefore to interrogate the framework within which those rules operate.

Data protection law presents itself as a technical and neutral regulatory framework. It does not reference gender, race or social position, it seemingly focuses on the processing of the rights of data subjects and the obligations of controllers. This type of approach is not neutral. A framework that defines harm in terms of identifiability, that locates the threshold of legal protection at the point of distribution rather than the point of creation and that balances the victim's right to erasure against abstract freedom of expression interests, is not neutral. It reflects a set of choices about whose experiences matter and whose harms count. As MacKinnon argued, the law sees the world from a male point of view and presents that point of view as objectivity itself.⁶⁵ Feminist theory exposes this perspective. Non-consensual deepfake pornography demands this kind of analysis precisely because its most serious harms such as representational injury, dignitary violation, the silencing of women from public life, are harms that a

⁶⁴ Carol Smart, *Feminism and the Power of Law* (Routledge 1989) 4.

⁶⁵ Catharine A MacKinnon, *Toward a Feminist Theory of the State* (Harvard University Press 1989) 162.

purely technical reading of the GDPR will not see. They fall outside the identifiability threshold and they go beyond distribution. A legal framework that fails to identify that it is a structural issue cannot be used as an answer to it. This thesis takes feminist legal theory seriously as an analytical method, which will be applied in the following chapters to specific provisions of EU data protection law. Because of that, it will demonstrate that a more appropriate legal response to the non-consensual deepfake pornography is feasible within the existing framework of EU fundamental rights.

One of the most crucial things to grasp is the fact that law is not a neutral instrument. It reflects and reproduces the power structures of the society that creates it.⁶⁶ Law fails women in the context of sexual exploitation.⁶⁷ This is, admittedly, one of the more contested strands of feminist legal theory but its diagnostic power for this specific harm is hard to avoid. MacKinnon's dominance theory holds that gender is hierarchy, maintained through social practices of which pornography is among the most powerful and that law reproduces rather than corrects this hierarchy.⁶⁸ Her central argument is that law is not a neutral arbiter standing above the social world.⁶⁹ This has a direct impact on how the legal framework responds or fails to respond to harms that primarily affect women. The system through which the law perceives the world was not designed to recognize it. The harm remains invisible from a legal perspective, it does not fit into existing categories, and it does not meet the required threshold. It is outweighed by competing interests and as the result women who experience it are left without the means to assert their rights.

For MacKinnon, pornography is a political practice and a mechanism of sex discrimination through which women are subordinated and reduced to objects for male use and gratification.⁷⁰ Pornography actively constructs and enforces subordination of women. It says that women exist for men's sexual purposes, that their bodies are available, that their consent is irrelevant and that their humanity is secondary to their function as sexual objects. This is not, MacKinnon argues, a matter of taste or offence. It is a matter of power.⁷¹

This argument maps directly and precisely onto non-consensual deepfake pornography. The creation of the content is not for women and it is not being made with women. It is being made from

⁶⁶ Catharine A MacKinnon, *Feminism Unmodified: Discourses on Life and Law* (Harvard University Press 1987) 147.

⁶⁷ *ibid*

⁶⁸ *ibid* 22

⁶⁹ Catharine A MacKinnon, *Toward a Feminist Theory of the State* (Harvard University Press 1989) 162.

⁷⁰ *ibid* 195

⁷¹ *ibid* 151

women, from their faces, their likenesses, their publicly available images and used as instruments of gratification, humiliation and control. The victim is not a participant. She is raw material and her consent has not merely been overlooked. It has been rendered irrelevant by a technology that does not require it and a legal framework that has not yet found a way to demand it. MacKinnon's analysis reveals this as a structural failure. Law has not failed to catch up with deepfake technology but to take seriously a harm whose primary victims are women.⁷² If MacKinnon is right and that law reflects existing power structures then the inadequacy of Article 17 GDPR as a remedy for non-consensual deepfake pornography is not simply a drafting oversight that better legislative technique could fix. It reflects the same structural blindness that has characterised law's engagement with sexual exploitation more broadly. A tendency to define harm in terms that exclude women's experiences, to locate legal protection at the point where male interests are threatened rather than where female dignity is violated and to resolve conflicts between competing rights in ways that consistently favour abstract expressive interests over concrete bodily ones.

If MacKinnon gives us the structural diagnosis, then Danielle Citron gives us the legal remedy. Citron's framework of sexual privacy is the theoretical bridge between the feminist critique of existing law and the doctrinal argument. Citron's central argument is that sexual privacy is a fundamental human interest, one that law has systematically and consistently under protected, because the legal system has historically failed to take seriously harms that fall predominantly on women.⁷³ Sexual privacy, as Citron defines it, is the right to control the sexual aspects of one's identity, body and intimate life.⁷⁴ It encompasses the right to decide who sees your body, who has access to information about your sexuality and how your sexual identity is represented to the world. It is a distinct and fundamental interest whose violation causes a specific and serious harm that cannot be reduced to reputational damage, emotional distress or any of the other categories through which law has traditionally attempted to capture it.⁷⁵ Legal frameworks, including the GDPR, have tended to approach the harms of non-consensual image-based abuse through the lens of privacy in the informational sense⁷⁶ as the exposure of facts or images that a person wished to keep private. This framing, while not wrong, is inadequate. It captures only part of what is happening. When a deepfake pornographic image is created without persons consent, something more

⁷² Catharine A MacKinnon, *Only Words* (Harvard University Press 1993) 15.

⁷³ Danielle Keats Citron, 'Sexual Privacy' (2019) 128 *Yale Law Journal* 1870, 1877.

⁷⁴ *ibid* 1880

⁷⁵ *ibid*

⁷⁶ See: Case C-131/12 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C:2014:317 The right to erasure, as interpreted by both national supervisory authorities and the Court of Justice of the European Union, has been understood primarily as a remedy for the continued processing of identifiable personal data without a lawful basis.

than private information is being exposed. Sexual identity is being fabricated, bodily autonomy overridden and right to define oneself on own terms is being stripped away. These are violations of sexual privacy in Citron's sense and they demand a legal response build for the nature and depth of the harm and not to the narrower question of whether identifiable information has been processed without a lawful basis.

Citron identifies three dimensions of sexual privacy violation that are directly relevant to non-consensual deepfake pornography.⁷⁷ The first is the violation of informational privacy - the exposure or fabrication of sexual content involving a person without their consent. The second is the violation of decisional privacy- the removal of a person's ability to make choices about their own sexual identity and how it is presented to others. The third is the violation of expressive privacy- the appropriation of a person's identity to construct a sexual narrative that they did not author and would never have consented to. Citron contends that existing legal frameworks need to be reinterpreted through the lens of sexual privacy if they are to provide adequate remedies for the harms of non-consensual image-based abuse.⁷⁸ Applying it to the deepfake porn, the right to erasure, as currently interpreted, may be remedy for informational harm. It addresses the processing and distribution of personal data without lawful basis. A reinterpretation informed by Citron's framework of sexual privacy would extend its reach to encompass decisional and expressive harm as well. Recognising that what is at stake is the restoration of a person's right to control their own sexual identity and digital representation. Citron also makes an argument that is important for understanding why the law has failed in the way that it has. The under protection of sexual privacy reflects a gendered devaluation of women's interests, a tendency to treat harms that fall predominantly on women as less serious, less urgent and less deserving of legal remedy than harms whose primary victims are men.⁷⁹ This argument connects directly to MacKinnon's structural critique and extends it into the specific domain of privacy law. Together, MacKinnon and Citron establish the theoretical foundation for the central claim of this thesis: that the inadequacy of Article 17 GDPR as a remedy for non-consensual deepfake pornography is a gendered gap and addressing it requires a fundamentally different understanding of what the right to erasure is for and whose interests it is designed to protect.

⁷⁷ Danielle Keats Citron, 'Sexual Privacy' (2019) 128 Yale Law Journal 1870, 1884.

⁷⁸ Danielle Keats Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* (W W Norton 2022) 97.

⁷⁹ Danielle Keats Citron, 'Sexual Privacy' (2019) 128 Yale Law Journal 1870, 1897.

At this point two assumptions that have been adopted in this thesis needs to be explained. In today's day and age, the nature of our digital identity is something more than just external pictures of ourselves. It constitutes as an integral part of who we are. Digital embodiment means that boundaries between the body and its representations has become increasingly blurred. Our social media profiles and digital presence in general became the extensions of our identity.⁸⁰ To fabricate a sexual representation of a person in digital space is to construct a false version of that person's embodied self and insert it into the world without their consent. This has direct legal consequences. If digital representations are understood as extensions of embodied identity, then the harm of non-consensual deepfake pornography cannot be adequately addressed by a framework concerned only with the processing and removal of information. It demands a framework attentive to bodily autonomy.

The feminist framework adopted in this thesis is not universalist. It does not treat women as a homogeneous category equally affected by the same harms in the same ways. The evidence presented in section 1.2 makes clear that this would be analytically inaccurate. The harm of non-consensual deepfake pornography is shaped by the intersection of gender with race, ethnicity, sexuality and other axes of structural disadvantage. This is the insight that Kimberlé Crenshaw's foundational concept of intersectionality provides. Systems of oppression interact and compound with each other, producing forms of harm that a single-axis analysis cannot capture.⁸¹

For the purposes of this thesis, the intersectional dimension of deepfake pornography manifests in two ways. As established in section 1.3, women of colour, trans women and non-binary individuals face compounded harms shaped by racial stereotype, transphobic stigma and other forms of structural discrimination that operate alongside and through gender-based harm. More importantly for the legal argument, the existing framework of EU data protection law is not equipped to recognise these compounded harms. A reinterpretation of Article 17 that attends only to gender without acknowledging the ways in which race and identity shape both the experience of harm and access to legal remedy would be incomplete. The feminist reinterpretation advanced in Chapter 5 is therefore intersectional in character and attentive to the full range of structural inequalities that non-consensual deepfake pornography both

⁸⁰ N Katherine Hayles, *How We Became Posthuman: Virtual Bodies in Cybernetics, Literature, and Informatics* (University of Chicago Press 1999) 3.

⁸¹ Kimberlé Crenshaw, 'Mapping the Margins: Intersectionality, Identity Politics, and Violence Against Women of Color' (1991) 43 *Stanford Law Review* 1241, 1244.

reflects and reinforces.⁸² That being said, I don't take this analysis as complete; a fuller intersectional account than this thesis can offer is clearly needed.

Combining feminist legal theory with doctrinal analysis of EU data protection law faces an obvious methodological challenge. Doctrinal analysis works from within the legal framework. It interprets provisions, analyses case law and identifies the boundaries of legal concepts as they currently exist. Feminist critique works from outside. It evaluates the framework against an external standard, exposes its assumptions while arguing for a different set of values. The position adopted here is that feminist theory is not being used to replace doctrinal analysis but to inform it. The two methods are not in competition, rather they operate at different levels. Doctrinal analysis establishes what Article 17 currently means and how it has been applied. Feminist theory reveals what that meaning assumes, what it excludes and what a more adequate reading would look like. As Bartlett has argued, feminist legal method does not stand outside law and condemn it from a distance.⁸³ It engages with legal materials on their own terms while insisting that those terms be evaluated against the experiences of those law claims to protect.⁸⁴ This methodological position has a specific legal foundation in EU law that makes it more than just normative. The Charter of Fundamental Rights requires that GDPR provisions be interpreted consistently with the values of human dignity, private life and gender equality enshrined in Articles 1, 7 and 23.⁸⁵ A feminist reinterpretation of Article 17 is an argument from within the legal framework. It asks only that the right to erasure be read in a manner consistent with the fundamental rights commitments that EU law has already made. That is a doctrinal argument that just also happens also to be a feminist one.

1.5 The Legal Gap: Why Existing Frameworks Fall Short

The harm described in the previous chapters is real, serious and affects mainly women and yet the current legislation does not provide these victims with sufficient support. Existing legal frameworks, whether criminal, civil, or regulatory, were not designed with synthetic media in mind. They were built

⁸² Kimberlé Crenshaw, 'Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics' (1989) University of Chicago Legal Forum 139.

⁸³ Katharine T Bartlett, 'Feminist Legal Methods' (1990) 103 Harvard Law Review 829, 831.

⁸⁴ *ibid*

⁸⁵ Charter of Fundamental Rights of the European Union [2012] OJ C326/391, arts 1, 7, 23.

around real images, traceable conduct and identifiable perpetrators. Deepfake pornography breaks each of these assumptions simultaneously and the result is a legal landscape in which the harm is visible, but the remedy is not.

It may seem that the most immediate response to the non-consensual deepfake pornography should be one facilitated by criminal law. In practice, however, criminal frameworks across EU member states are poorly equipped to address it. Most existing legislation targeting image-based sexual abuse was designed for real intimate images which presupposes an original photograph or recording that was created consensually and subsequently distributed without consent.⁸⁶ Deepfakes require neither.⁸⁷ Some jurisdictions have begun to respond, e.g. the United Kingdom's Online Safety Act 2023 introduced a specific offence of sharing intimate deepfake images⁸⁸, and several EU member states are in the process of legislative reform.⁸⁹ Nevertheless, the coverage remains fragmented, enforcement is inconsistent and criminal law functions after the harm has already been done.⁹⁰ It punishes perpetrators, but it does not restore victims.

Civil frameworks fare no better. Defamation law, the most obvious candidate, requires the claimant to establish that a false statement of fact has damaged their reputation. A deepfake perpetrator can argue that the image is obviously fabricated and therefore not capable of being understood as a statement of fact.⁹¹ Copyright law offers no meaningful protection either. It protects the creator of an image not the person depicted in it, which in the deepfake context means that whatever intellectual property rights subsist in the fabricated content belong to the perpetrator.⁹² Harassment law requires a course of conduct and may not capture the creation or single distribution of a deepfake image. Data protection law outside the GDPR framework is similarly limited. None of these frameworks was designed to recognise representational injury or dignitary harm.

It is within this context of comprehensive civil and criminal inadequacy that the GDPR emerges as the most promising existing legal tool available to victims of non-consensual deepfake pornography.

⁸⁶ Clare McGlynn and Erika Rackley, 'Image-Based Sexual Abuse' (2017) 37 Oxford Journal of Legal Studies 534, 536.

⁸⁷ Robert Chesney and Danielle Keats Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753, 1760.

⁸⁸ Online Safety Act 2023, s 188.

⁸⁹ Law Commission, Intimate Image Abuse: A Final Report (Law Com No 407, 2022).

⁹⁰ *ibid* 12

⁹¹ Robert Chesney and Danielle Keats Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753, 1760.

⁹² David Harris, 'Deepfakes: False Pornography is Here and the Law Cannot Protect You' (2019) 17 Duke Law and Technology Review 99, 112.

Its potential is genuine. The regulation applies to the processing of personal data, imposes obligations on controllers and gives data subjects the right to demand erasure under Article 17. In principle, a victim could invoke these provisions to demand the removal of deepfake content from platforms, search engines and hosting services. The right to be forgotten, established in *Google Spain* and codified in Article 17, provides a legal mechanism that no criminal or civil framework currently matches in terms of practical reach and enforceability.⁹³ However, the GDPR's potential as a remedy for non-consensual deepfake pornography is constrained at every level by the interpretive framework within which it currently works.

The first limitation concerns the definition of personal data under Article 4(1). The right to erasure can only be invoked where the content in question constitutes personal data. Whether an AI-generated image of a recognisable individual meets this threshold is not settled. The synthetic nature of deepfakes complicates the identifiability analysis in ways that existing CJEU case law does not directly address. If a deepfake image does not qualify as personal data, the entire GDPR framework falls away.

The second gap concerns the scope and application of Article 17 itself. Even where personal data is established, the right to erasure as currently interpreted is a remedy for informational harm. It does not recognise the deeper harms of representational injury, dignitary violation and loss of narrative control. A right to erasure that can order the removal of content but cannot name or remedy the harm that content represents is a partial remedy at best.

The third and most structurally significant gap concerns the exceptions to erasure under Article 17(3). Even where a victim successfully establishes that deepfake content constitutes personal data and invokes the right to erasure, that right can be defeated by competing interests. The balancing framework through which these competing interests are resolved has, as MacKinnon's analysis predicts, tended to favour abstract expressive interests over the concrete bodily and dignitary harms suffered by victims. This is not a neutral outcome; it is a structural bias that feminist reinterpretation must address.

Taken together, these three gaps define the legal problem that the remainder of this work addresses. The GDPR is not the wrong tool. It is a powerful and far-reaching regulatory framework with genuine potential to provide meaningful remedies for victims of non-consensual deepfake pornography. But that potential will remain unrealised so long as the framework is interpreted through a purely technical and gender-blind lens. What is needed is a reinterpretation of existing provisions that takes

⁹³ Case C-131/12 *Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González* [2014] ECLI:EU:C: 2014:317.

seriously the harms established in this chapter and the feminist theoretical framework developed to analyse them.

Chapter II Synthetic Identity and the Limits of Personal Data

2.1 The concept of personal data under article 4(1) GDPR

The scope of the GDPR is defined by the concept of personal data. Where data does not meet that definition, the regulation does not apply and its protections cannot be invoked.⁹⁴ The right to erasure under Article 17 is no exception, it can be used only where the content in question constitutes personal data within the meaning of article 4 (1) GDPR.⁹⁵ Whether a deepfake image meets that threshold is therefore the gateway question on which the entire regulatory response depends. Article 4(1) of the GDPR defines Personal Data as:

“any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.”⁹⁶

The legal elements of this definition can therefore be named as the criterion of identifiability, the concept of “relating to” the term “any information” and “natural person”.

The phrase "any information" is deliberately broad. It is not limited to information that is sensitive, private or harmful.⁹⁷ This includes both objective and subjective information (facts, opinions, assessments and analyses), provided that the other elements of the definition are met.⁹⁸ This applies to any information whose processing poses a risk to the rights and freedoms of the data subject. As confirmed by the Article 29 Working Party in its landmark opinion on the concept of personal data, the word “any” indicates that this definition should be interpreted broadly.⁹⁹ Such an approach ensures

⁹⁴ 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) [2016] OJ L119/1.

⁹⁵ Finck M and Pallas F, 'They Who Must Not Be Identified - Distinguishing Personal from Non-Personal Data Under the GDPR' (2020) 10 International Data Privacy Law 11, 12.

⁹⁶ GDPR art 4(1).

⁹⁷ Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data (WP 136, 2007) 6.

⁹⁸ *ibid*

⁹⁹ *ibid*

consistency with the overarching objective of the Regulation, which is the protection of natural persons.¹⁰⁰

The phrase "natural person" requires less elaboration in the present context. It simply excludes legal persons from the protection of the regulation and as victims of non-consensual deepfake pornography are self-evidently natural persons, this element requires no further analysis.

An element of particular significance for this analysis, is the identifiability criterion. Person is identifiable, according to the definition, where they can be identified "directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, genetic, mental, economic, cultural or social identity of that natural person."¹⁰¹ Identification does not need to be direct and it is sufficient that a person could be identified by combining the data in question with other available information. This principle of indirect identifiability significantly expands the reach of the definition beyond data that names or obviously points to a person.¹⁰² A photograph from which a face can be recognised, a voice recording from which a speaker can be identified, a combination of physical characteristics that distinguishes one individual from others, can constitute personal data even where they contain no explicit identifying information.¹⁰³ Some characteristics are so distinctive that a person can be identified with little effort, but in other situations, combining details at a categorical level (age group, regional origin, etc.) can also prove quite decisive, especially if additional information is available.¹⁰⁴

Recital 26 GDPR specifies that in assessing identifiability, account should be taken of "all the means reasonably likely to be used" to identify the person, "either by the controller or by another person."¹⁰⁵ The standard is whether the identification is reasonably possible given the means available. This notion of reasonable likelihood opens the door to an argument that a synthetic image from which a person could be identified by reasonable means constitutes personal data even where that identification requires additional steps or the combination of multiple data sources. While identifiability determines whether a person falls within the scope of the definition at all, the "relating to" criterion determines

¹⁰⁰ *ibid* 4

¹⁰¹ GDPR, art 4(1).

¹⁰² Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data (WP 136, 2007) 13.

¹⁰³ Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data (WP 136, 2007) 13; Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland [2016] ECLI:EU:C:2016:779, para 49.

¹⁰⁴ Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data (WP 136, 2007) 13.

¹⁰⁵ GDPR, Recital 26.

whether a specific piece of information is sufficiently connected to that person to constitute their personal data.

The term “relating to” has also been broadly interpreted by the Article 29 Working Party. Three alternative criteria were identified based on which information can be considered to relate to a specific individual: the content-based criterion, the purpose-based criterion and the effect-based criterion.¹⁰⁶ Information has a content element where it is directly about the person. It has a purpose element where it is used with the intention of evaluating, treating or influencing the person in some way as well as a result element where its processing is likely to have an impact on that person's rights or interests, even if the information is not directly about them. This tripartite interpretation is significant for the deepfake analysis because it suggests that an image does not need to contain directly identifying information to relate to a person, it is sufficient that it is about them or has consequences for them. Another aspect directly related to deepfakes is the fact that the “result” element broadens the concept of personal data to include information whose processing affects the interests of the individual, regardless of whether that information would traditionally be understood as relating to that person. A deepfake image that causes psychological, reputational and dignitary harm to the person depicted in it clearly has a result element in relation to that person.¹⁰⁷ Its processing affects their interests in the most direct and serious way imaginable.

Beyond the general framework of identifiability and relational connection, a specific category of data deserves separate treatment in this setting. Biometric data under Article 4(14) and Article 9 GDPR is defined as "personal data resulting from specific technical processing relating to the physical or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopy data."¹⁰⁸ It is subject to enhanced protection under Article 9, which prohibits its processing in the absence of explicit consent or another specified lawful basis.¹⁰⁹ Deepfakes are generated from biometric data. The technology works by processing the victim's facial geometry, physical characteristics and/ or vocal biometrics, to produce a synthetic representation that replicates their appearance with sufficient accuracy to be convincing. Regardless of any doubts concerning the status of content generated using deepfake technology under Article 4(1), the input data—the biometric data obtained from publicly available photographs of the victim and used to create synthetic

¹⁰⁶ Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data (WP 136, 2007), 10.

¹⁰⁷ *ibid* 11

¹⁰⁸ GDPR, art 4(14); art 9.

¹⁰⁹ GDPR, art 9(1).

content, undoubtedly constitutes special category personal data.¹¹⁰ This issue is of significant importance because it establishes the minimum level of protection provided for in the GDPR, which exists independently of any analysis of traceability. Even under the most restrictive interpretation of Article 4(1), the processing of biometric data for the purpose of creating deepfake content is subject to the strictest protective provisions of that regulation.¹¹¹

Lastly, the purposive character of the definition must be addressed. The definition of personal data in Article 4(1) is a purposive concept, interpreted in light of the GDPR's foundational objective of protecting the fundamental rights and freedoms of natural persons in connection with the processing of their data.¹¹² This means that where a narrow technical reading of the definition would exclude data whose processing clearly poses risks to those rights and freedoms, a purposive reading is required.¹¹³ The GDPR's definitional framework must be understood as serving the regulation's broader normative commitments.¹¹⁴ The question is not whether a deepfake image fits neatly within the technical parameters of Article 4(1) as traditionally understood. The question is whether a reading of Article 4(1) that excludes synthetic media from its scope is consistent with the GDPR's fundamental rights objectives.

2.2 Court of Justice of the European Union's case law on personal data and its implications

It is essential to note that the definitional framework described above does not operate in isolation from its context. It has been interpreted and applied by the Court of Justice of the European Union in a series of rulings that have gradually expanded the concept of personal data and confirmed its purpose-driven and technology-neutral nature. Three cases are of particular relevance at this stage of the analysis: *Lindqvist*, *Breyer* and *Nowak*. None of them directly concerns synthetic media, but together they form a

¹¹⁰ Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data (WP 136, 2007) 8; GDPR, arts 4(14), 9(1).

¹¹¹ GDPR, arts 4(14), 9(1); Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015); see also Article 29 Data Protection Working Party, Opinion 3/2012 on Developments in Biometric Technologies (WP 193, 2012) 8.

¹¹² GDPR, Recital 1; Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data (WP 136, 2007) 4.

¹¹³ Regulation (EU) 2016/679 (GDPR), Recital 1; Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data (WP 136, 2007) 4.

¹¹⁴ Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data (WP 136, 2007) 25.

set of interpretive principles that directly influence whether and to what extent deepfakes fall within the scope of Article 4(1).

Lindqvist was decided under the Data Protection Directive 95/46/EC not the GDPR, but its interpretive principles remain authoritative under the current framework given the definitional continuity between the two instruments.¹¹⁵ The case concerned a Swedish woman who had posted information about her colleagues on a parish website, including references to one colleague's medical condition. The Court held that posting information about named and identifiable individuals on an internet page constitutes the processing of personal data within the meaning of EU data protection law.¹¹⁶ The significance of *Lindqvist* for the present analysis lies in the principle it confirms: the concept of personal data is broad, technology-inclusive and not limited to traditional forms of information. The Court did not ask whether the internet was the kind of medium the legislature had envisaged when drafting the Directive. It asked whether the information related to identified or identifiable natural persons and answered affirmatively. The fact that synthetic media was not contemplated when the GDPR was drafted does not place it beyond the definition's reach any more than the internet placed parish websites beyond the Directive's reach in *Lindqvist*.

Patrick Breyer v Bundesrepublik Deutschland is the most important case for the deepfake identifiability argument and therefore requires a more detailed treatment. The case concerned whether dynamic IP addresses constitute personal data. The website operator argued that they did not, because it could not itself identify the user from the IP address alone without obtaining additional information from the internet service provider. The Court rejected this argument.¹¹⁷ It held that a dynamic IP address constitutes personal data where the website operator has the legal means to obtain the additional information needed to identify the user, even if that information is held by a third party.¹¹⁸ The crucial principle is that indirect identifiability is sufficient and it is not necessary that the controller alone possesses all the information required for identification. It is sufficient that identification is reasonably possible through combination of the data with other available information, whether held by the controller or by any other person.¹¹⁹ Two aspects of this principle are directly applicable to the deepfake context. The reasonable likelihood standard applies to any third party who might view the image. A deepfake

¹¹⁵ Case C-101/01 *Bodil Lindqvist* [2003] ECLI:EU:C: 2003:596, para 24; the definitional continuity between Directive 95/46/EC and the GDPR is confirmed in GDPR, Recital 9.

¹¹⁶ Case C-101/01 para 27.

¹¹⁷ Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] ECLI:EU:C: 2016:779, para 33.

¹¹⁸ *ibid* para 49

¹¹⁹ *ibid* para 42

perpetrator who generates a synthetic image of a recognisable person cannot argue that the image does not constitute personal data simply because they themselves may not know the victim's identity. If a reasonable viewer could identify the person depicted, the identifiability criterion is satisfied.¹²⁰ Furthermore, the Court confirmed that the assessment of reasonable likelihood must take account of all available means, including technical developments during the period for which the data will be processed.¹²¹ In the deepfake context, where facial recognition technology is becoming increasingly sophisticated and accessible, the means available to identify individuals from synthetic images are expanding. This dynamic reading of identifiability supports a broad application of the definition to deepfake output.

Peter Nowak v Data Protection Commissioner works on a different level than the *Breyer* case. It is concerned with whether examination scripts completed by a candidate constitute personal data of that candidate. The data controller argued that they did not. The scripts were documents produced by the candidate in a professional examination context and their primary purpose was to assess the candidate's knowledge rather than to contain information about them. The Court disagreed.¹²² It held that examination scripts constitute personal data of the candidate because they reflect their knowledge, competence and intellectual capacity, information that relates to one through both the content and result elements of the "relating to" criterion.¹²³ The result element was particularly significant: the scripts related to the candidate because their processing, specifically their evaluation by the examiner, would have direct consequences for their professional future. The accuracy or conventional character of the information was irrelevant to this analysis. *Nowak* confirms that the "relating to" criterion extends to novel and unconventional forms of information that do not fit the traditional model of personal data as a file containing facts about a named individual. An examination script is not, in the obvious sense, a record about a person. It is a record produced by a person in a specific context. A deepfake image is similarly unconventional. It is a fabrication generated from and directed at a person.¹²⁴ *Nowak* supports the argument that this unconventional character does not place it beyond the definition's reach. *Nowak* also confirms that the result element functions independently of the accuracy or conventional character of the information. The examination scripts related to the candidate because their processing had consequences

¹²⁰ *ibid* para 43

¹²¹ GDPR, Recital 26; Breyer para 46

¹²² Case C-434/16 *Peter Nowak v Data Protection Commissioner* [2017] ECLI:EU:C: 2017:994, para 34.

¹²³ *ibid* para 35

¹²⁴ *ibid* para 21

for him. A deepfake image relates to the victim because its creation and circulation have devastating consequences for that person, which permits the result element argument advanced in section 2.3.

Read together, these three cases establish interpretive principles that bear directly on the personal data status of deepfakes. The definition of personal data is broad, purposive and technology-neutral, it extends to novel forms of information and new technological contexts without requiring explicit legislative intervention.¹²⁵ Indirect identifiability through combination of data with other available information is sufficient, and the reasonable likelihood standard applies to any person and not just to the controller alone.¹²⁶ The "relating to" criterion is interpreted expansively to include information that relates to a person through the result element rather than through direct identification alone.¹²⁷ The accuracy of the information is irrelevant to its status as personal data.¹²⁸ Each of these principles supports the argument that deepfake pornography engages the GDPR's definitional framework. However, it is crucial to note that none of these cases directly addressed synthetic media. The CJEU has not yet ruled on whether an AI-generated image of a recognisable person constitutes personal data and the doctrinal gap that results is real. The principles established in *Lindqvist*, *Breyer* and *Nowak* support an affirmative answer but do not compel one.

2.3 The challenge of deepfakes: hybrid form of data

The principles established in the preceding section provide a foundation. Whether they are adequate for the specific challenge deepfakes present is another question entirely. Deepfakes do not fit neatly into existing categories of personal data because they occupy a legally uncomfortable middle ground that existing doctrine was not designed to address. They are a hybrid form of data. Understanding what that means and what are the consequences of this classification, is the purpose of this section.

¹²⁵ Case C-101/01 Bodil Lindqvist [2003] ECLI:EU:C: 2003:596, para 24; Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland [2016] ECLI:EU:C:2016:779, para 49; Case C-434/16 Peter Nowak v Data Protection Commissioner [2017] ECLI:EU:C:2017:994, para 34.

¹²⁶ Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland [2016] ECLI:EU:C: 2016:779, paras 44-49; GDPR, Recital 26.

¹²⁷ Case C-434/16 Peter Nowak v Data Protection Commissioner [2017] ECLI:EU:C: 2017:994, paras 34-35; Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data (WP 136, 2007) 10-11.

¹²⁸ Case C-434/16 Peter Nowak v Data Protection Commissioner [2017] ECLI:EU:C: 2017:994, para 34; Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data (WP 136, 2007) 6.

The clearest and most doctrinally secure basis for GDPR coverage of non-consensual deepfake pornography does not concern the synthetic image at all. It concerns the data used to generate it. As established in section 2.1, deepfakes are produced by processing the victim's biometric data extracted from publicly available photographs and recordings. That processing engages Article 9 GDPR directly. Biometric data processed for the purpose of uniquely identifying a natural person is a special category of personal data subject to the regulation's most stringent protective provisions.¹²⁹ Its processing is prohibited in the absence of explicit consent or another specified lawful basis.¹³⁰ The perpetrator of deepfake pornography created without the victim's consent cannot avoid this conclusion by arguing that the source images were publicly available because public availability does not imply consent to the processing of data for the purpose of creating synthetic content of a sexual nature. A photo posted on a social media profile is shared for social purposes, such as networking or communication. Regardless of the purpose, it is certainly not intended to be shared for the purpose of obtaining biometric data and creating sexual content. The aim for which biometric data are processed is just as important as the fact of their processing itself, and the processing of publicly available biometric data for the purpose of creating pornographic content without the consent of the data subjects does not fall within any of the categories of lawful processing set forth in Article 9(2).¹³¹ This argument provides an independent and unassailable basis for GDPR coverage that exists regardless of how the personal data question is answered.

The status of the synthetic image itself, the deepfake output, under article 4(1) is indeed more difficult, and it would be untruthful to present it any other way. The difficulty arises from the hybrid nature of the of the output. A deepfake image is simultaneously derived from a real person and fabricated. It contains no information that the person provided while depicting conduct that never occurred. It is, in the most literal sense, false. Can false information about a real person constitute personal data about that person? Article 29 Working Party's foundational opinion on the concept of personal data, says yes.¹³² The Working Party stated explicitly that "it is not necessary for the information to be considered as personal data that it is true or proven."¹³³ Data protection rules already contemplate the possibility that information is incorrect and provide rights of rectification accordingly. A deepfake image is false

¹²⁹ GDPR, art 4(14); Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data (WP 136, 2007) 8.

¹³⁰ GDPR, art 9(1).

¹³¹ GDPR, art 9(2).

¹³² Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data (WP 136, 2007) 6.

¹³³ *ibid*

information about a real person. But false information about a real person is still information about that person and it is information whose processing can cause that person serious and documented harm. The more difficult question is whether the person depicted in the deepfake can be identified from the output and whether identification is even the right threshold for protection.

The identifiability analysis applied to deepfake output produces different results depending on the specific characteristics of the image and the victim. For a convincingly realistic deepfake of a recognisable individual such as a public figure, a celebrity, a politician etc. the image was generated to resemble them, it does resemble them and a reasonable observer would identify them from it. This satisfies the indirect identifiability criterion established in Recital 26- identification is reasonably possible by means available to any person who views the image.¹³⁴ In such cases the output constitutes personal data on the identifiability basis alone. For less publicly recognisable individuals the analysis is more uncertain. Where a victim has a limited online presence and the deepfake image does not contain additional contextual identifiers, the reasonable likelihood of identification may be harder to establish. This is a genuine doctrinal gap and acknowledging it is important. It reveals that the identifiability criterion, applied in its traditional form, produces inconsistent results depending on the victim's public profile rather than on the nature or severity of the harm she has suffered. A framework that offers stronger protection to celebrities than to private individuals is not a framework designed with victims' interests at its centre.

The result element of the Article 29 Working Party's tripartite “relating to” test, introduced in section 2.1, provides a more consistent and arguably more appropriate basis for establishing that deepfake output constitutes personal data. As established in section 2.1, information relates to a person where its processing is likely to have an impact on their rights and interests, regardless of whether the information directly identifies them.¹³⁵ A deepfake pornographic image of a person, even if they cannot be immediately identified from it, clearly satisfies this criterion. Its creation and circulation cause psychological, reputational, dignitary and professional harm of the kind documented in section 1.3. It affects the victim's interests directly and seriously. It relates to her because it is about her, generated from her and directed at her with the consequences falling directly on her alone. This basis for coverage is particularly significant because it operates independently of identifiability. It asks whether the image's processing has consequences for rights of the victim. In the context of deepfakes, when a harm is inherent

¹³⁴ GDPR, Recital 26; Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland [2016] ECLI:EU:C:2016:779, para 49.

¹³⁵ Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data (WP 136, 2007) 11.

in the creation of the content, not contingent on its distribution or the victim's recognisability, the answer will always be yes. This is precisely the insight that Öhman's concept of representational injury captures at the theoretical level and that the result element of the "relating to" test captures at the doctrinal level.¹³⁶

The processing of biometric input data to generate synthetic sexual content without consent violates Article 9 regardless of the output's status while said output relates to the victim within the meaning of Article 4(1) through the result element of the Working Party's tripartite test, independently of whether she can be identified from the image. The identifiability of the output, which applies where the victim is sufficiently recognisable, produces inconsistent results across different categories of victim. The question of which analytical pathway provides the most secure and consistent basis for GDPR engagement is therefore unresolved. As section 2.4 will demonstrate, the inconsistency is itself a symptom of a deeper inadequacy in the traditional identifiability framework, one that a purposive and feminist reinterpretation of Article 4(1) must address.

2.4 The inadequacy of traditional identifiability framework

The traditional identifiability framework is inadequate from a structural point. It reflects a series of choices regarding which harms matter and whose experiences the law is meant to protect. The issue with identifiability as the primary gateway to GDPR protection is not even the fact that it produces uncertain results in the deepfake context, the problem is that it asks the wrong question. The identifiability criterion is designed around informational harm. It poses the questions whether a person can be identified or singled out from the group or can a link be established between this data and this specific person. These are the right questions to ask for a system designed to process documentation, files, and databases, but they might be insufficient with synthetic intimate imagery.

As Öhman's concept of representational injury establishes, and as section 1.3 documented at length, the harm of non-consensual deepfake pornography does not begin when the victim is identified. It begins when the image is created.¹³⁷ The violation inheres in the act of constructing a false sexual representation of a person without their knowledge or consent, regardless of whether anyone ever

¹³⁶ Carl Öhman, 'Introducing the Pervert's Dilemma: A Contribution to the Critique of Deepfake Pornography' (2020) 22 Ethics and Information Technology 133.

¹³⁷ Carl Öhman, 'Introducing the Pervert's Dilemma: A Contribution to the Critique of Deepfake Pornography' (2020) 22 Ethics and Information Technology 133, 136.

connects that representation to them. A framework that withholds protection until identification occurs is a framework that arrives after the harm has already been done and offers nothing to the victim whose image exists but has not yet been traced back to her. This is particularly damaging for private individuals, the category of victims for whom the identifiability threshold is most likely to fail. A convincingly realistic deepfake of a celebrity or public figure will almost certainly satisfy the indirect identifiability criterion because a reasonable viewer would recognise her. But any person with limited online presence may not be immediately recognisable from the image even to most viewers. The identifiability framework offers her weaker protection precisely because she is less well known. Stronger protection for the already privileged and weaker protection for the already vulnerable is a structural failure.¹³⁸

It reflects the same gendered blindness that MacKinnon identified in law's engagement with sexual exploitation more broadly.¹³⁹ It reveals the choice about what kind of harm the law recognises and whose experiences it takes seriously. A framework built for informational harm is a framework designed around a concept of privacy as secrecy. As Cohen argued, privacy is about the ability to develop and control one's own identity over time.¹⁴⁰ The identifiability threshold protects the former while leaving the latter entirely unprotected.

The harms that fall outside the identifiability threshold, such as dignitary harm and the fabrication of false sexual self, are exactly the harms that fall predominantly on women. Citron's framework of sexual privacy makes this connection explicit: the systematic under protection of sexual privacy reflects a gendered devaluation of women's interests.¹⁴¹ A definition of personal data that requires identification before protection is engaged is a definition that systematically fails the victims of non-consensual deepfake pornography, not because it was designed to fail them, but because it was not designed with them in mind at all.

The solution is not to abandon the identifiability framework entirely. It is to ensure that it does not operate as the sole gateway to protection. The purposive character of GDPR requires that Article 4(1) be interpreted in a manner consistent with the regulation's fundamental rights objectives.¹⁴² A reading that excludes synthetic media from the definition's scope on the grounds that the output may not be

¹³⁸ Michelle Finck and Frank Pallas, 'They Who Must Not Be Identified: Distinguishing Personal from Non-Personal Data Under the GDPR' (2020) 10 International Data Privacy Law 11, 14.

¹³⁹ Catharine A MacKinnon, *Toward a Feminist Theory of the State* (Harvard University Press 1989) 162.

¹⁴⁰ Julie E Cohen, 'What Privacy Is For' 126 Harvard Law Review 1904 (2013), 103.

¹⁴¹ Danielle Keats Citron, 'Sexual Privacy' (2019) 128 Yale Law Journal 1870, 1875.

¹⁴² GDPR, Recital 1; Charter of Fundamental Rights of the European Union [2012] OJ C326/391, arts 1, 7, 8.

immediately identifiable is inconsistent with those objectives where the processing of that media causes serious harm to the rights and freedoms of the person depicted. The result element of the Article 29 Working Party's tripartite "relating to" test provides the doctrinal mechanism for a broader reading that does not depend on identification at all.¹⁴³ As already noted in sections 2.1 and 2.3, a deepfake image is linked to the victim through the result, regardless of whether the victim can be identified in it, because its creation has devastating consequences for the victim's rights and interests. This is simply a consistent application of an interpretive principle already established by the Working Party and confirmed by the Court in *Nowak*. What it requires is a willingness to treat the result element as a primary basis for the "relating to" criterion, asking whether the processing affects her rights. It might be objected that treating the result element as a primary basis for the "relating to" criterion risks extending the definition of personal data too broadly, capturing almost any information whose processing has consequences for someone. The Article 29 Working Party itself cautioned that the scope of data protection rules should not be overstretched.¹⁴⁴ This concern is legitimate in the abstract however, with deepfakes it does not hold. The result element is being invoked here to capture consequences that are certain, severe and directly traceable to the processing of the victim's biometric data such as psychological trauma, reputational destruction, dignitary violation and the permanent alteration of a woman's digital identity without her consent. These are the kind of serious harm to fundamental rights and freedoms that the GDPR was designed to address.¹⁴⁵

This reinterpretation also has a grounding in the concept of digital embodiment. If it is an extension of our embodied identity, then a fabricated sexual representation of a person's digital embodiment is a fabrication about that person, and about her in the most intimate and damaging sense, regardless of whether it identifies her in the conventional informational sense.¹⁴⁶ The definition of personal data must evolve to reflect this understanding of digital identity or it will continue to offer protection designed for conception of selfhood that the digital age has already rendered obsolete.

The practical consequences of this reinterpretation are direct and significant. Victims of non-consensual deepfake pornography would have standing to invoke the GDPR's full framework of rights, regardless of whether they are immediately identifiable from the content. The processing of biometric

¹⁴³ Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data (WP 136, 2007) 10-11.

¹⁴⁴ Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data (WP 136, 2007) 5.

¹⁴⁵ GDPR, Recital 1; Charter of Fundamental Rights of the European Union [2012] OJ C326/391, art 8.

¹⁴⁶ N Katherine Hayles, *How We Became Posthuman: Virtual Bodies in Cybernetics, Literature, and Informatics* (University of Chicago Press 1999) 3; Julie E Cohen, 'What Privacy Is For' 126 *Harvard Law Review* 1904(2013), 103.

data to generate deepfake content engages Article 9's would enhance protection framework independently of the output question, an independent and unassailable basis for GDPR coverage that exists regardless of how the identifiability question is resolved. Platform controllers and search engines would be subject to erasure obligations that cannot be avoided by pointing to the fabricated character of the content or the victim's limited public profile.

Chapter III The Right to Erasure: Scope, Application and Limitations

3.1 Development, Conditions Triggering and Obligations of Controllers under article 17 GDPR

The right to be forgotten under Article 17 GDPR emerged from Article 12(b) of the Data Protection Directive 95/46/EC, which gave data subjects the right to demand rectification, erasure or blocking of data whose processing did not comply with the Directive.¹⁴⁷ That provision was limited in scope and inconsistently applied across Member States. The GDPR transformed it into a codified, directly applicable right to erasure with clearly defined triggering conditions and controller obligations. The right to be forgotten reflects a deliberate legislative choice to give data subjects meaningful control over their personal data in the digital age.¹⁴⁸ This choice affects how the law should be interpreted and what can be anticipated from it in the context of non-consensual deepfake pornography.

Article 17(1) GDPR provides that a data subject has the right to obtain erasure of personal data concerning them without undue delay where one of six grounds is met.¹⁴⁹ Not all six are equally relevant to the deepfake context. Three merit specific attention.

Article 17(1)(a): the personal data is no longer necessary in relation to the purpose for which it was collected or otherwise processed.¹⁵⁰ In the deepfake context this ground has limited utility, because the data was not collected for a legitimate purpose that eventually loses its validity. From the very beginning, it has been collected with the intent to cause harm. The legal grounds arising from the lapse of a legitimate purpose do not unequivocally clarify a situation in which the creation of the content was never justified.

Article 17(1)(b): the data subject withdraws consent and there is no other lawful basis for processing.¹⁵¹ This ground is more promising but faces a specific difficulty here. Article 17(1)(b) is designed for situations where consent was once given and is subsequently withdrawn. In deepfake context consent was never given and a criterion of a presupposed prior consensual relationship between

¹⁴⁷ Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data [1995] OJ L281/31, art 12(b).

¹⁴⁸ GDPR, Recital 65.

¹⁴⁹ GDPR, art 17(1).

¹⁵⁰ *ibid* (a)

¹⁵¹ *ibid* (b)

the data subject and the processing, does not exist. Applying this ground requires an argument that the absence of consent is equivalent to its withdrawal, an argument that is available but not straightforward.

Article 17(1)(d): the personal data have been unlawfully processed, is the most important criterion in the context of this thesis.¹⁵² If deepfake content constitutes personal data processed without a legal basis, then its processing is unlawful within the meaning of Article 17(1)(d), and on this basis, its erasure may be requested without the need to demonstrate prior consent or the expiry of a legitimate purpose.¹⁵³ This is the most doctrinally secure triggering condition for victims of non-consensual deepfake pornography.

Once a triggering condition is established, Article 17(1) imposes an obligation on the controller to erase the personal data without undue delay.¹⁵⁴ Article 17(2) extends this obligation. Where the controller has made the personal data public, it must take reasonable steps to inform other controllers processing the data that the data subject has requested erasure.¹⁵⁵ This notification obligation is significant with deepfakes because it potentially extends the reach of a single erasure request beyond the platform originally hosting the content to other platforms that have shared or reproduced it. In practice, however, its reach is limited by what counts as "reasonable steps"- a standard that is undefined in the regulation and has been interpreted narrowly by supervisory authorities in the online content context.¹⁵⁶

Article 17 imposes obligations on so called "data controllers". In the context of deepfakes, determining who qualifies as the data controller is no simple matter. The perpetrator who created the content, the platform hosting it, the search engine indexing it and the content delivery network distributing it may all be involved in the processing of the same synthetic image and each occupies a different position in the regulatory framework. *Google Spain* established that search engines are controllers for the purposes of the right to be forgotten and can be required to delist content on request.¹⁵⁷ But delisting by a search engine does not delete the underlying content and the platform hosting that content is a separate controller subject to separate obligations. Where content may be hosted across multiple platforms in multiple jurisdictions simultaneously, the fragmentation of controller responsibility creates significant practical obstacles for victims seeking comprehensive erasure. The controller

¹⁵² *ibid* (d)

¹⁵³ *ibid*

¹⁵⁴ GDPR art. 17 (1).

¹⁵⁵ GDPR, art 17(2).

¹⁵⁶ European Data Protection Board, Guidelines 5/2019 on the Criteria of the Right to Be Forgotten in the Search Engines Cases Under the GDPR (2020) 7.

¹⁵⁷ *Google Spain*, para 41.

framework under Article 17, while theoretically capable of reaching the full chain of processing, was not designed with the distributed and anonymised character of deepfake distribution in mind.

3.2 Delisting Versus Deletion: A Critical Distinction

The right to erasure sounds comprehensive. The word “erasure” implies complete removal and elimination of content from the digital environment. What Article 17 has delivered in practice is something considerably more limited. The distinction between delisting and deletion is the difference between making content harder to find and making it cease to exist. For victims of non-consensual deepfake pornography, it is the difference between a partial remedy and a meaningful one.

Google Spain established that search engines are controllers within the meaning of EU data protection law and can be required to remove links to content from search results on request.¹⁵⁸ This was a landmark decision. For the first time, data subjects had a directly enforceable mechanism to limit the discoverability of information about them online. But what the judgment delivered is delisting, the removal of the link from the search engine. The content remains on the web and can still be accessed directly through its URL. It can still be shared through messaging applications, social media platforms and peer-to-peer networks as well as be indexed by search engines in other jurisdictions. Delisting from Google reduces the likelihood of a casual user stumbling across content through a conventional search. It does nothing to prevent targeted distribution or access by anyone who already has the link.¹⁵⁹ This is not to say that delisting is without value. For the ordinary internet user, Google is effectively the only gateway to the internet. With a global search market share consistently exceeding 90%, content that does not appear in Google results is, for most people, content that does not exist.¹⁶⁰ A successful delisting request therefore achieves something genuinely significant, by removing the content from the primary means by which most people discover information online. For a victim concerned about casual discovery by employers, colleagues, friends or acquaintances, delisting provides real and immediate protection.

¹⁵⁸ *ibid*

¹⁵⁹ Tambiama Madiaga, 'European Court of Justice Limits the Territorial Scope of the "Right to Be Forgotten"' (European Parliamentary Research Service, PE 642.273, October 2019) [https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/642273/EPRS_ATA\(2019\)642273_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/642273/EPRS_ATA(2019)642273_EN.pdf) accessed 29 April 2026.

¹⁶⁰ StatCounter, Search Engine Market Share Worldwide (StatCounter Global Stats, 2024) <https://gs.statcounter.com/search-engine-market-share> accessed 29 April 2026.

The limitation becomes acute, however, when the threat is targeted distribution. Deepfake content is not typically discovered through general internet searches but rather distributed through dedicated pornographic platforms¹⁶¹, encrypted messaging applications¹⁶² and closed online communities that operate entirely outside the reach of search engine delisting.¹⁶³ A successful delisting request removes the content from one layer of discoverability while leaving it entirely intact at every other level.

The more meaningful remedy for deepfake victims is deletion from the hosting platform directly. Article 17(1)(d) imposes an erasure obligation on the controller hosting the content. Platforms hosting deepfake pornography are controllers within the meaning of the GDPR.¹⁶⁴ In principle, a victim can invoke Article 17(1)(d) to demand deletion of the content at source. In practice, however, this remedy faces obstacles that significantly limit its effectiveness.

The first obstacle is jurisdictional. Many platforms hosting non-consensual deepfake content operate outside the EU and are therefore beyond the direct enforcement reach of the GDPR. While Article 3(2) extends the GDPR's territorial scope to controllers outside the EU who process data in connection with the offering of goods or services to EU data subjects¹⁶⁵, enforcing erasure obligations against non-EU platforms in practice requires cooperation from national supervisory authorities and courts in the platform's home jurisdiction. This kind of cooperation in practice seems mostly unavailable. The second obstacle is the definitional one already examined in Chapter 2. A platform disputing that deepfake content constitutes personal data, arguing that the synthetic image does not identify the victim, can resist a deletion request on the grounds that Article 17 does not apply at all. The purposive reinterpretation of Article 4(1) argued in Chapter 2 addresses this obstacle at the doctrinal level, but until that reinterpretation is adopted by supervisory authorities or courts, platforms retain the ability to use definitional uncertainty as a shield against compliance. The third obstacle is strictly practical. Even where a platform complies with a deletion request, the content may already have been reproduced and distributed across dozens of other platforms simultaneously. Article 17(2)'s notification obligation does not compel those other controllers to delete. It requires only that they be informed. The EDPB has

¹⁶¹ Henry Ajder and others, *The State of Deepfakes: Landscape, Threats, and Impact* (Deeptrace 2019) https://regmedia.co.uk/2019/10/08/deepfake_report.pdf accessed 11 April 2026.

¹⁶² Robert Chesney and Danielle Keats Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 *California Law Review* 1753.

¹⁶³ Europol, *Facing Reality? Law Enforcement and the Challenge of Deepfakes* (Europol Innovation Lab 2022), 20.

¹⁶⁴ GDPR, art. 4(7); Case C-131/12 *Google Spain* para 41.

¹⁶⁵ GDPR art. 3 (2).

interpreted "reasonable steps" narrowly in the online content context, and the notification obligation has not in practice operated as a mechanism for coordinated cross-platform deletion.¹⁶⁶

A further constraint on the effectiveness of the delisting remedy concerns its territorial reach. In *Google LLC v CNIL*, the Court held that EU law does not require global delisting.¹⁶⁷ The obligation extends only to EU versions of the search engine not to its worldwide results.¹⁶⁸ Content delisted from EU search results remains accessible through non-EU versions of the same search engine and through search engines based outside the EU entirely. In a digital environment where content crosses jurisdictional boundaries instantaneously and permanently, a territorially limited delisting obligation provides protection geared for a pre-digital understanding of how information travels. However significant, it would be unrealistic to credit the EU with a global jurisdiction.

Given both the distinction between the delisting and the removal of content, as well as the jurisdictional obstacles hindering the removal of content from platforms and the territorial restrictions on the removal of content from search results, Article 17, as currently interpreted, appears to be a remedy whose scope is significantly narrower than the scale of the harm it is may address in the context of deepfakes. What is needed is comprehensive deletion.

3.3 Procedural and Practical Limitations

The limitations set out in section 3.1 and section 3.2 do not exhaust the difficulties victims of non-consensual deepfake pornography that invoke article 17 GDPR face. The situation is exacerbated by several procedural and practical obstacles that hinder the system's operation at every stage, from the submission of an application through to enforcement. Each of these obstacle's stem more from interpretative choices and implementation failures.

Under the current framework, the practical burden of invoking Article 17 falls almost entirely on the data subject. They must identify the relevant controller, establish that the content constitutes personal data, demonstrate that a triggering condition under Article 17(1) is met, formulate a legally coherent

¹⁶⁶ European Data Protection Board, Guidelines 5/2019 on the Criteria of the Right to Be Forgotten in the Search Engines Cases Under the GDPR (2020) 7.

¹⁶⁷ Case C-507/17 *Google LLC v Commission nationale de l'informatique et des libertés (CNIL)* [2019] ECLI:EU:C:2019:772, para 64.

¹⁶⁸ *ibid*

erasure request and submit it through mechanisms that vary widely across platforms and Member States.¹⁶⁹ For the victims of non-consensual deepfake porn, each of these steps involves barriers that are disproportionate to the harm suffered. They must repeatedly contact the platform hosting content whose very existence causes them deep distress and whose operators may not be interested in complying with the law. In many cases, they must do so without legal assistance, at a time when the psychological effects of the harm suffered are at their most acute.¹⁷⁰ This procedural burden reflects the lack of specific procedural guidelines regarding deepfake cases and the fact that supervisory authorities have not established accessible complaint mechanisms that take into account the particular vulnerability of victims of the misuse of synthetic images of an intimate nature.¹⁷¹

A controller receiving an erasure request must verify the identity of the person making it before complying.¹⁷² It is a legitimate safeguard against fraudulent requests but at the same time one that creates a specific and underappreciated difficulty in the deepfake context. The victim is required to identify herself to the platform hosting synthetic intimate content about her to demand its removal.¹⁷³ In cases where the deepfake was created by a former partner, a stalker or a perpetrator who is monitoring her behaviour, this identification requirement may expose her to further harm. Meanwhile, the perpetrators and platforms against whom she is making the request frequently operate under conditions of anonymity or pseudonymity that place no equivalent burden on them.¹⁷⁴ The verification requirement functions asymmetrically, reflecting a procedural framework designed more with disputes over commercial data processing in mind than with gender-based digital violence.¹⁷⁵ It requires the victim to disclose their identity, whilst ensuring the perpetrator's anonymity.

Article 57(1)(f) GDPR requires supervisory authorities to handle data subject complaints and to investigate matters relevant to the regulation's application.¹⁷⁶ In principle, a victim who cannot obtain

¹⁶⁹ GDPR, art 17(1); European Data Protection Board, Guidelines 5/2019 on the Criteria of the Right to Be Forgotten in the Search Engines Cases Under the GDPR (2020) 5.

¹⁷⁰ Danielle Keats Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* (W W Norton 2022) 41.

¹⁷¹ European Data Protection Board, Guidelines 5/2019 on the Criteria of the Right to Be Forgotten in the Search Engines Cases Under the GDPR (2020); Danielle Keats Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* (W W Norton 2022) 41–43.

¹⁷² GDPR art. 12 (6).

¹⁷³ *ibid*

¹⁷⁴ Aleksandra Kuczerawy and Jef Ausloos, 'From Notice-and-Takedown to Notice-and-Delist: Implementing Google Spain' (2016) 14 *Colorado Technology Law Journal* 219, 231–232.

¹⁷⁵ Danielle Keats Citron, 'Sexual Privacy' (2019) 128 *Yale Law Journal* 1870, 1874; Danielle Keats Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* (W W Norton 2022) 41.

¹⁷⁶ GDPR, arts 57(1)(f), 58(2).

compliance from a platform through a direct erasure request can file a complaint with her national supervisory authority and request that it exercise its enforcement powers.¹⁷⁷ In practice, enforcement by supervisory authorities in individual image-based abuse cases has been inconsistent and slow. Resources are disproportionately directed towards large-scale commercial data processing and systemic violations and many supervisory authorities have not developed specific procedures or priority frameworks for deepfake complaints.¹⁷⁸ This gap in enforcement reflects prioritisation of decisions that should be re-examined as part of a feminist reinterpretation, considering the gravity and gender-specific nature of the harm caused by deepfakes.

Article 17(1) requires erasure without undue delay. No binding guidance specifies what this means in practice and in the absence of specific guidance supervisory authorities have not imposed demanding timelines on controllers responding to deepfake erasure requests.¹⁷⁹ This is of immense significance in the context of deepfakes, given the speed at which synthetic content spreads once it enters online distribution networks. By the time a erasure request has been processed, verified, approved and enforced the content may have been viewed and downloaded millions of times, replicated across dozens of platforms and shared within closed communication networks to which no single removal order has access. The harm, in Öhman's terms, is not remedied by subsequent removal of content that has already constituted the victim's representation in the minds of everyone who has seen it.¹⁸⁰ A stricter interpretation of the “without undue delay” principle, taking into account the exponential spread of synthetic intimate content, could significantly narrow this gap even within the framework of the current legislation.

There is also a genuine structural obstacle that cannot be overcome even through a new interpretation of Article 17. This concerns the sharing of deepfake content on platforms based on blockchain technology or fully decentralised platforms, where there is no identifiable entity responsible for data processing nor any technical mechanisms available to enable its removal. This is an honest limitation and should not be understated. But it should also not be overstated. The majority of non-consensual deepfake content is hosted on conventional platforms subject to GDPR jurisdiction where Article 17 can in principle operate effectively. The blockchain problem affects a subset of cases.

¹⁷⁷ *ibid* arts 77(1), 58(2).

¹⁷⁸ Danielle Keats Citron, *The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age* (W W Norton 2022) 41–43.

¹⁷⁹ GDPR, art 17(1); EDPB Guidelines 5/2019 (n 1) 7.

¹⁸⁰ Carl Öhman, 'Introducing the Pervert's Dilemma: A Contribution to the Critique of Deepfake Pornography' (2020) 22 *Ethics and Information Technology* 133, 136.

Allowing it to define the assessment of the framework's overall utility would be to permit the exception to define the rule.

These procedural and practical limitations compound the substantive inadequacies. They constitute the gap between what Article 17 currently delivers and what victims of non-consensual deepfake pornography need. But they are also, in the most important cases, the product of interpretive choices, enforcement priorities and implementation failures and not just irremediable structural defects.

3.4 The Remedial Value of Legal Recognition

The limitations established across sections 3.1, 3.2 and 3.3 are real and should not be minimised. Article 17, in its current interpretation, does not deliver complete erasure of non-consensual deepfake pornography. It does not reach every controller in every jurisdiction, it does not bridge the gap between delisting and deletion, and it does not relieve the data subject of procedural burdens that fall disproportionately on those least equipped to bear them. The victims will in many cases find this legal framework insufficient. Any defence of the merits of this framework must begin by acknowledging this fact. Recognising this does not, however, mean abandoning the entire framework. The argument put forward here is that legal recognition under Article 17 has a remedial value, regardless of whether complete erasure can be achieved in each case. This value is significant enough that it is worth retaining and reinterpreting this framework, rather than replacing it.

The first issue concerns the very nature of legal recognition. If Article 17 named non-consensual synthetic intimate imagery as personal data the processing of which the data subject has the right to terminate, it would do something that neither criminal law nor tort law performs in quite the same way.¹⁸¹ Criminal law responds to wrongs through sanctions and tort law responds through compensation.¹⁸² Article 17 establishes the data subject's status as a rights-holder with a positive entitlement to control and not just as complainant seeking redress for a wrong already done.¹⁸³ This shift, from victim to rights-holder, has a dignitary value that is not contingent on the practical effectiveness of enforcement in any given case.

¹⁸¹ Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015) 89–94.

¹⁸² Peter Cane, *The Anatomy of Tort Law* (Hart Publishing 1997) 27–32.

¹⁸³ Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harvard University Press 2014) 226–229.

Waldron's analysis of dignity as status rather than as the absence of indignity is instructive here.¹⁸⁴ Recognition of a person as a rights-holder is constitutive of dignity.¹⁸⁵ To be the holder of a right is to occupy a status that the legal system acknowledges and that other actors must respect.¹⁸⁶ The right does not become valuable only when it is enforced, it carries value through the recognition it confers.¹⁸⁷ This understanding is can be applied to the right to data protection, which the CJEU has consistently treated as a freestanding fundamental right under Article 8 of the Charter not just an instrumental adjunct to privacy under Article 7.¹⁸⁸ A parallel argument can be developed in the context of image- based sexual abuse.¹⁸⁹ The legal system's refusal to recognise the harm of non-consensual intimate imagery as cognisable harm is itself a form of harm, a denial of personhood that compounded the underlying violation.¹⁹⁰ The corresponding act of legal recognition reverses that denial by transforming the legal status of the person from one whose harm the law fails to see into one whose harm the law names and grants standing to remedy.¹⁹¹ For the victim of non-consensual deepfake pornography, this transformation is meaningful even where the practical remedy remains imperfect.¹⁹²

Next consideration concerns the structural effects of legal recognition on the conduct of controllers. Even where individual erasure requests fail, the existence of the right shapes the regulatory environment within which platforms operate.¹⁹³ Article 17 imposes binding obligations on controllers to respond to requests within defined timeframes, to demonstrate lawful basis for continued processing and to face supervisory enforcement for non-compliance.¹⁹⁴ These obligations shape how platforms design their systems, train their moderators and allocate their resources, regardless of how any individual request is resolved. This is what Lessig characterised as the regulatory function which is law's capacity to shape the technical environment.¹⁹⁵ Hildebrandt has developed the argument in the specific context of data-driven environments, arguing that legal protection must increasingly be inscribed into the design of

¹⁸⁴ Jeremy Waldron, *Dignity, Rank, and Rights* (University of California, Berkeley, April 21-23, 2009) 210.

¹⁸⁵ *ibid*

¹⁸⁶ *ibid* 209

¹⁸⁷ *ibid*

¹⁸⁸ Case C-92/09 Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen [2010] ECLI:EU:C:2010:662, paras 47–48; Charter of Fundamental Rights of the European Union [2012] OJ C326/391, art 8.

¹⁸⁹ Mary Anne Franks, 'Unwilling Avatars: Idealism and Discrimination in Cyberspace' (2011) 20 *Columbia Journal of Gender and Law* 224.

¹⁹⁰ *ibid* 236–238.

¹⁹¹ *ibid* 260.

¹⁹² Danielle Keats Citron, 'Sexual Privacy' (2019) 128 *Yale Law Journal* 1870, 1939–1942.

¹⁹³ Lawrence Lessig, *Code: Version 2.0* (Basic Books 2006) 121–125.

¹⁹⁴ GDPR, art 12(3), art 6(1), art 9(2), art 58(2).

¹⁹⁵ Lawrence Lessig, *Code: Version 2.0* (Basic Books 2006) 5–8 and 121–125.

technical systems and not rely solely on ex post enforcement.¹⁹⁶ Cohen has applied this framework directly to GDPR obligations, observing that data protection law works as a structural constraint on the design of informational infrastructures.¹⁹⁷ For the victim of non-consensual deepfake pornography, this architectural function matters because it creates regulatory pressure that may, over time, make platforms less hospitable to deepfake content even where individual requests against existing content remain difficult. Platforms operating under the shadow of Article 17 must build systems capable of receiving, processing and acting on erasure requests at scale. They must employ moderators trained to identify the relevant content as well as establish procedures that can withstand supervisory scrutiny. None of this guarantees that any request succeeds, but it shifts the equilibrium in which platforms operate.

The remedial value of Article 17 depends on how it is interpreted. The argument across sections 3.1 to 3.3 has not been that Article 17 is incapable of providing meaningful remedy - it is that the current interpretation under-delivers on the framework's potential. A purposive and feminist reinterpretation, attentive to the dignitary harm established in Chapter 1 can substantially expand the practical remedy that Article 17 delivers. The remedial value of legal recognition is a function of interpretive choices which are revisable. None of this is to suggest that Article 17 is sufficient on its own. The legal response to non-consensual deepfake pornography requires multiple frameworks operating in concert: image-based abuse legislation, criminal law reform, the AI Act's emerging requirements on synthetic media and supervisory and judicial interpretation of fundamental rights obligations under the Charter. The argument here is that Article 17 has a distinctive contribution to make alongside these other frameworks, not that it can replace them. It is rights-based and it functions at the level of platform architecture rather than only at the level of individual enforcement. Other frameworks deliver other things, but no other framework delivers recognition of the data subject's positive entitlement to control her digital representation in the form Article 17 provides.

¹⁹⁶ Mireille Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Edward Elgar 2015) 219.

¹⁹⁷ Julie E Cohen, *Between Truth and Power: The Legal Constructions of Informational Capitalism* (Oxford University Press 2019) 262-263.

Chapter IV When Expression Trumps Dignity: The Structural Bias of the Exceptions Framework

4.1 The Exceptions Under Article 17(3): An Overview

The right to be forgotten under Article 17(1) GDPR is not absolute, in its paragraph 3 there are five grounds on which the right does not apply. The practical reach of the right depends as much on how those grounds are applied as on the scope of the right itself.¹⁹⁸ A right that may be restricted by broadly interpreted exceptions differs in practice from a right where exceptions are interpreted narrowly. These exceptions determine what the right delivers in the deepfake context as much as in any other.

The right does not apply where processing is necessary for the exercise of the right to freedom of expression and information, for compliance with a legal obligation under Union or Member State law or for the performance of a task carried out in the public interest, for reasons of public interest in the area of public health, for archiving in the public interest, scientific or historical research, or statistical purposes or for the establishment, exercise or defence of legal claims.¹⁹⁹ Platforms hosting deepfake content are most likely to invoke the freedom of expression exception under Article 17(3)(a), framing the content as expressive material whose removal would interfere with the rights of users.²⁰⁰ Where deepfake content depicts public figures or has been characterised as commentary on matters of public concern, the public interest exception under Article 17(3)(d), especially the archiving and research limbs, may be invoked. The remaining grounds are unlikely to bear directly on the deepfake context and will be addressed only where they have residual relevance.

The Court of Justice has developed a balancing framework for applying the exceptions. The framework was established in *Google Spain* and refined in *GC and Others* and later in *TU and RE v Google*.²⁰¹ It requires courts to weigh the data subject's right to erasure against the competing interest invoked under the exception, on a case-by-case basis.²⁰² Both interests are treated as fundamental rights of presumptively equal weight at the outset. The right to data protection under Article 8 of the Charter

¹⁹⁸ GDPR art. 17(3).

¹⁹⁹ *ibid* Art 17(3)(a) -(e).

²⁰⁰ Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford University Press 2015) 256–260.

²⁰¹ Case C-131/12 *Google Spain*; Case C-136/17 *GC and Others*.; Case C-460/20 *TU and RE v Google LLC* [2022] ECLI:EU:C:2022:962.

²⁰² *Google Spain* paras 81, 99; *GC and Others*, paras 57, 66.

on one side, the competing interest, most often freedom of expression under Article 11, on the other. The balance is determined by the specific circumstances of each case.²⁰³ The CJEU has identified factors relevant to that balance, including the nature of the data, the role of the data subject in public life, the purpose of the processing and the public interest in continued availability of the information.²⁰⁴

This framework is presented as neutral. It treats conflicting rights as commensurable. The balance is determined by the circumstances of each case and the methodology is available to all parties on an equal footing. That presentation doesn't hold up here.

4.2 Freedom of Expression and the Balancing Framework

The right to be forgotten works through a structured balancing exercise that the Court of Justice has developed across three Grand Chamber decisions: *Google Spain*, *GC and Others*, and *TU and RE v Google*. Each judgment has contributed a distinct element to the framework. The architecture these cases establish is the doctrinal terrain on which any future deepfake-related Article 17 dispute could be resolved.

Google Spain established that the right to erasure is not absolute and must be balanced against the rights and interests of others. The court held that, as a general rule, the data subject's rights under Articles 7 and 8 of the Charter override both the economic interest of the search engine operator and the public interest in finding the information through a search on the data subject's name.²⁰⁵ This rule admits exceptions depending on the nature of the information, its sensitivity for the data subject's private life and the public's interest in having access to that information.²⁰⁶ The court identified the role of the data subject in public life as a particularly significant factor: where the data subject plays a role in public life, the interference with their fundamental rights may be justified by the preponderant interest of the general public in access to the information.²⁰⁷

GC and Others confirmed and refined this framework. The court held that the rights conferred by Articles 7 and 8 of the Charter are not absolute and must be considered in relation to their function in

²⁰³ Charter, arts 8, 11; *Google Spain* paras 81; *GC and Others* paras 57,58.

²⁰⁴ *Google Spain* para 81; *GC and Others* paras 66,68,75.

²⁰⁵ *Google Spain* para 81.

²⁰⁶ *ibid*

²⁰⁷ *ibid*

society and balanced against other fundamental rights in accordance with the principle of proportionality.²⁰⁸ Article 52(1) of the Charter requires that any limitation on the exercise of the rights and freedoms recognised by the Charter must be provided for by law, respect the essence of those rights and freedoms and be subject to the principle of proportionality.²⁰⁹ Within this structure, the court identified the relevant factors for the balance: the nature of the information in question, its sensitivity for the data subject's private life, the interest of the public in having access to the information and the role of the data subject in public life.²¹⁰

Across those cases, the CJEU has identified a set of factors that by interacting with each other structure the balancing exercise under Article 17(3)(a). Case law leaves the question of their relative weight to be determined on a case-by-case basis by national courts and supervisory authorities.²¹¹ The first factor is the nature of the information in question. *Google Spain* and *GC and Others* both treat the nature of the information as a primary consideration, with sensitive personal data within the meaning of Article 9 GDPR receiving heightened protection.²¹² Where the information falls within the special categories of personal data, the data subject's interest in erasure is presumed to outweigh the public interest in access, subject to exceptions for journalistic purposes and other public interest considerations.²¹³ Another factor is the public interest in having access to the information. The case law treats this factor as carrying significant analytical weight, with the court repeatedly emphasising that the public interest in access is what justifies, in appropriate cases, the continued availability of information that interferes with the data subject's rights.²¹⁴ The factor encompasses the public interest in journalistic reporting, in access to judicial records, in scrutiny of public figures and in historical and archival information. Another factor is the role of the data subject in public life. The case law treats public figures as having a reduced expectation of privacy in matters relating to their public role.²¹⁵ The court ruled that the factor's weight depends on the nature and significance of the public role and on the relationship between the information sought to be erased and the exercise of that role.²¹⁶ The last factor is the time

²⁰⁸ *GC and Others* para 57.

²⁰⁹ *ibid* para 58

²¹⁰ *ibid* para 66

²¹¹ The case law does not establish a hierarchy among the factors. National courts and supervisory authorities are required to apply the framework on a case-by-case basis, taking account of the specific circumstances of each case. See *Google Spain* para 81; *GC and Others* paras 66-68.

²¹² *GC and Others* paras 44-47.

²¹³ *ibid* paras 64-69.

²¹⁴ *Google Spain* para 81; *TU and RE v Google* para 64.

²¹⁵ *Google Spain* para 81.

²¹⁶ *GC and Others* paras 44-47.

elapsed since publication and the continued relevance of the information. *Google Spain* held that information may become inadequate, irrelevant, or no longer relevant over time, supporting a stronger claim to erasure.²¹⁷ This factor reflects the framework's origins in cases concerning information whose contemporary relevance had diminished since original publication.

TU and RE v Google extended the framework established by the two previously described cases to thumbnail images displayed by search engines. The court held that thumbnails require a separate balancing exercise distinct from the assessment of the articles they accompany, because the display of thumbnails on a search results page constitutes a particularly significant interference with the data subject's rights to private life and personal data.²¹⁸ The most important factor in this separate balance is the "informative value" of the image, considered together with any text element accompanying the thumbnail that is capable of casting light on its informative value for the public.²¹⁹ The case extended the framework's analytical reach to visual content as a distinct category but did so within the same structural logic: the framework asks about the informative value of the image and weighs that value against the data subject's rights, treating the image as content whose removal must be justified against expressive interests.

The case law as it currently stands does not address fabricated content as distinct from authentic content. *Google Spain*, *GC and Others*, and *TU and RE v Google* all concerned content whose accuracy, relevance, or contextual appropriateness was disputed, but whose status as a depiction of the data subject was not. The framework has not developed a factor for synthetic content, has not addressed deepfakes and has not provided guidance on how the existing factors apply to imagery that depicts the data subject in events that did not occur. The CJEU has not been asked to address these questions. National courts in EU Member States have not yet referred Article 17 preliminary references concerning synthetic intimate imagery, in part because deepfake pornography litigation has tended to proceed through criminal law, image rights, defamation, and platform governance regimes rather than through the right to erasure.

²¹⁷ *Google Spain* para 92-94.

²¹⁸ *TU and RE v Google* paras 95-97.

²¹⁹ *ibid* paras 105-108

4.3 The Structural Bias Problem

The balancing framework set out in the sections above is presented as neutral, treating the rights being weighed up as comparable, with the outcome of the case directly dependent on the circumstances of that specific case. This presentation does not survive application to non-consensual deepfake pornography. The framework's structure produces systematically skewed analytical positions in the deepfake context and the pattern of those skews is not random.²²⁰ It reflects features of the framework that feminist legal theory has identified in legal thought more broadly.²²¹

Article 17(3)(a) treats the competing interest as freedom of expression and information, a fundamental right of presumptively equal weight, to the data subject's rights under Articles 7 and 8 of the Charter.²²² Where the speech is authentic communication on a matter of public concern, that presumption is defensible.²²³ It breaks down once the content is fabricated synthetic intimate imagery whose only connection to expression is that someone uploaded it to a platform. The framework, as currently constituted, applies the presumption regardless of whether the underlying content has any genuine expressive character.²²⁴ A deepfake video of a recognisable woman in a non-consensual sexual scenario is treated, for the purposes of the balancing analysis, as expressive material whose removal must be justified by countervailing considerations. The presumption is that the content is expression. The framework treats "the public interest in continued availability of the information" as a factor weighing against erasure.²²⁵ The same difficulty recurs with the public-interest factor. A genuine public concern such as public figure's financial history, or the criminal record of someone seeking a position of trust, plainly justifies continued availability, non-consensual synthetic intimate imagery does not.²²⁶ Yet the factor offers no way to exclude it, because it assumes that anything circulating in public discourse carries some claim to public-interest protection. The deepfake context exposes the limits of that assumption. Public figures within the framework are treated as having a reduced expectation of privacy in matters

²²⁰ Catharine A MacKinnon, *Toward a Feminist Theory of the State* (Harvard University Press 1989) ch. 13.

²²¹ *ibid*

²²² Charter of Fundamental Rights of the European Union [2012] OJ C326/391, arts 8, 11; *Google Spain* para 81; *GC and Others* paras 57, 58.

²²³ *Google Spain* paras 80-85.

²²⁴ The framework does not provide any doctrinal mechanism for distinguishing authentic from fabricated content within the freedom of expression analysis. See further section 4.2 above on the absence of any deepfake-specific factor in the existing case law.

²²⁵ *Google Spain* para 81; *GC and Others* para 66.

²²⁶ Neil M. Richards, *Intellectual Privacy: Civil Liberties and Information in Digital Age* (New York: Oxford University Press, 2014).

relating to their public role.²²⁷ The role-in-public-life factor fails in the same direction. It is sound as applied to authentic information about how a public figure exercises her functions, but it cannot distinguish that from fabricated sexual content that exploits her visibility as a pretext for targeting.²²⁸ A woman who has chosen to enter the public life, has not, because of that choice, accepted reduced protection against the production and circulation of synthetic content depicting her in non-consensual sexual acts. Or at least she shouldn't have to. The framework has no doctrinal mechanism for marking that distinction.

These features reflect a deeper structural trait of the legal framework itself. It was developed within a legal tradition that regards freedom of expression as a value in its own right and places the burden of justification on those who seek to restrict it, rather than on those who defend the value of the statement in question.²²⁹ MacKinnon's analysis of pornography and law is the most direct articulation of why this matters. Her argument in *Only Words* is that pornography is not speech in the sense that traditional free expression doctrine protects. It is itself an act of subordination and treating it as speech presupposes the very thing the speech-versus-act distinction is supposed to evaluate.²³⁰ The doctrinal structures differ significantly between the US and EU systems, particularly given the proportionality-based architecture of EU fundamental rights law. Nevertheless, the underlying presumption identified by MacKinnon that sexually exploitative material is initially treated as protected expression, appears in modified form within the Article 17 balancing framework.²³¹ The presumption that synthetic intimate imagery is expressive material, requiring case-specific justification for its removal, presupposes that such imagery has the character of expression rather than the character of harm. This structure risks predetermining aspects of the balancing exercise before the specific harms of synthetic sexual content are fully considered.

The connection to MacKinnon's broader argument in *Toward a Feminist Theory of the State* sharpens the point. Her claim is that law treats male perspectives as objective and that legal categories developed within male-dominated frameworks fail to recognise harms that fall disproportionately on women.²³² The balancing framework under Article 17(3)(a) is not exempt from this dynamic. The

²²⁷ *Google Spain* para 81; *GC and Others* para 66.

²²⁸ Danielle Keats Citron, 'Sexual Privacy' (2019) 128 *Yale Law Journal* 1870, 1925–1932.

²²⁹ Catharine A MacKinnon, *Only Words* (Harvard University Press 1993) 71–77.

²³⁰ *ibid* 9–14

²³¹ *ibid* 21–30, The conceptual move that MacKinnon identifies operates across jurisdictional contexts because it concerns the underlying conception of expression rather than the specific doctrinal vocabulary in any particular legal system.

²³² Catharine A MacKinnon, *Toward a Feminist Theory of the State* (Harvard University Press 1989) ch. 13.

presumption of expressive value, the treatment of public interest and the role-in-public-life factor were all developed in cases involving the kind of information dispute that arises in male-dominated public contexts.²³³ The cases that established the framework did not involve, and could not have involved, the harm at issue here. *Google Spain* concerned outdated commercial information about a real estate auction, *GC and Others* concerned journalistic reporting and judicial records and *TU and RE v Google* concerned thumbnail images of investment managers in articles disputed for inaccuracy. The most recent of these cases is the closest the framework has come to addressing visual content as a distinct category, but it did so within an analytical structure that presupposed authentic depiction of the applicants. As already mentioned, no CJEU case has yet addressed synthetic intimate imagery. The framework is not failing to recognise a harm it can see, it has simply never been asked to see it and the categories it has developed in cases it has been asked to see were never built to register what deepfake pornography does to its victims.

Citron and Franks have developed parallel arguments in the specifically Anglo-American context of image-based abuse.²³⁴ Citron's analysis of cyber civil rights observes that legal frameworks treating non-consensual intimate imagery as expression rather than as harm reflect the same structural blindness MacKinnon identifies in earlier feminist scholarship.²³⁵ Franks's work on unwilling avatars develops the argument specifically in relation to digital embodiment and consent.²³⁶ The argument advanced here applies the same analytical lens to the EU balancing framework. The doctrinal vocabulary differs but the structural feature is the same.

It might be objected that the framework is genuinely neutral, that the case-specific factors can weigh heavily enough on a victim's side to produce a favourable outcome. The difficulty is that those factors are never assessed from neutral ground. The question of how heavily to weight a victim's dignitary harm against the expressive interest in the content is not asked from a neutral position.²³⁷ It is asked from a position that has already constructed the content as expressive material. That position places the burden of justification on the victim seeking removal and not on the platform defending continued circulation.²³⁸

²³³ See Case *Google Spain* paras 14–17; *GC and Others* paras 19–24.

²³⁴ Danielle Citron, *Hate Crimes in Cyberspace* (Harvard University Press 2014) 121–128, Mary Anne Franks, 'Unwilling Avatars: Idealism and Discrimination in Cyberspace' (2011) 20 *Columbia Journal of Gender and Law* 224, 248–250.

²³⁵ Danielle Citron, *Hate Crimes in Cyberspace* (Harvard University Press 2014) 218–221.

²³⁶ Mary Anne Franks, 'Unwilling Avatars: Idealism and Discrimination in Cyberspace' (2011) 20 *Columbia Journal of Gender and Law* 224, 248–250.

²³⁷ Catharine A MacKinnon, *Toward a Feminist Theory of the State* (Harvard University Press 1989) 238.

²³⁸ Catharine A MacKinnon, *Only Words* (Harvard University Press 1993) 71–77; see also Frederick Schauer, *Free Speech: A Philosophical Enquiry* (Cambridge University Press 1982) 136–148.

Framework's structure systematically disadvantages victims by determining the analytical position from which the balancing is conducted. This leaves a question the framework cannot comfortably answer: what expressive value can the creation and circulation of a fabricated sexual video of an identifiable person plausibly carry and what exactly does its author express that free-expression doctrine was built to protect?

4.4 Public Interest Across the Framework

The structural critique developed in section 4.3 operated on Article 17(3)(a), the freedom of expression exception. The framework's qualifying provisions extend beyond that single exception. Public interest considerations also enter the right to erasure analysis through Article 9(2)(g) GDPR, which permits the processing of sensitive personal data where necessary "for reasons of substantial public interest," and through Article 85 GDPR, which requires Member States to reconcile data protection rights with freedom of expression and information for processing carried out for journalistic, academic, artistic, or literary purposes.²³⁹ Both provisions interact with Article 17 by providing grounds on which public interest claims can defeat or qualify erasure rights.

The CJEU's most extensive engagement with these provisions in the right to be forgotten context is *GC and Others*. The case held that the prohibitions and restrictions on processing sensitive personal data under Article 9 GDPR apply to search engine operators in the same way they apply to any other controller, but that the operator's responsibility is engaged at the verification stage following a request for de-referencing, not at the indexing stage.²⁴⁰ Within that framework, the court held that even where the underlying publication serves journalistic purposes within the meaning of Article 85, the balancing exercise between the data subject's rights and the freedom of information must still be conducted and the balance can favour erasure where the data subject's rights outweigh the public interest in access.²⁴¹ The substantive content of that balance is structured by the same factors identified in section 4.2.

The presumption of expressive value reappears as a presumption that journalistic publication, or publication invoking substantial public interest, has the character of legitimate public discourse. The treatment of public interest as a factor weighing against erasure is similar. The framework asks whether

²³⁹ GDPR arts 9(2)(g), 85.

²⁴⁰ *GC and Others* paras 41-44.

²⁴¹ *ibid* paras 65-69

the public has an interest in continued access to the information, not whether the content depicts events that occurred. The role-in-public-life factor is identical across both Article 17(3)(a) and the public interest provisions, with public figures held to a reduced expectation of privacy in matters relating to their public role regardless of which exception is invoked.

Each of these features carries the same presupposition that section 4.3 surfaced. The public interest provisions, like the freedom of expression exception, were built to govern disputes about how information about real events should be made available. The journalistic exception under Article 85 was developed in cases involving reporting on actual occurrences. The substantial public interest ground under Article 9(2)(g) presupposes that the sensitive data being processed bears on something that exists. Neither provision has a way of telling the difference between something that happened and something that was invented to look like it did. The framework's treatment of public interest, across all three doctrinal sites, is built for a presupposition of authentic depiction. Whether erasure is resisted under the freedom of expression exception, the substantial public interest ground, or the journalistic exception, the framework asks the data subject to justify removal against an analytical structure that presupposes the content is what content has historically been: a depiction of something that exists. Non-consensual synthetic intimate imagery does not fit that presupposition and the framework's qualifying provisions, taken together, contain no analytical resources to register that fact.

This conclusion sets the doctrinal scene for the reinterpretation chapter 5 develops. The argument is not that the framework's particular factors should be reweighted, but that the framework as a whole carries presuppositions that cannot accommodate the harm at issue without substantive reinterpretation.

Chapter V Feminist Reinterpretation of Article 17: Dignity, Consent, and Digital Integrity

5.1 The Charter as the Interpretive Foundation

The Charter of Fundamental Rights of the European Union is the constitutional foundation within which the GDPR functions and against which it must be interpreted. This is the framework within which the GDPR was adopted and within which its provisions, including those reinterpreted in this chapter, must be read.

Since the entry into force of the Treaty of Lisbon on 1 December 2009, the Charter has had "the same legal value as the Treaties" under Article 6(1) of the Treaty on European Union.²⁴² Article 51(1) of the Charter provides that its provisions are addressed to the institutions, bodies, offices and agencies of the Union and to the Member States when they are implementing Union law.²⁴³ The GDPR, as an instrument of Union law adopted by Union institutions, is therefore subject to the Charter both at the point of its adoption and at the point of its interpretation and application by Member State authorities and national courts. The principle of consistent interpretation requires that EU secondary legislation be interpreted, so far as possible, in conformity with the Charter.²⁴⁴ Where there are differing interpretations of a provision of the GDPR, preference should be given to the interpretation that is more consistent with the rights enshrined in the Charter. This principle is a constitutional requirement arising from the hierarchical relationship between primary and secondary EU law and from the Charter's status as primary law.

The CJEU has applied this requirement in the data protection context across a substantial body of case law. In *Volker und Markus Schecke*, the Grand Chamber held that the validity of EU secondary legislation must be assessed against Articles 7 and 8 of the Charter and that the proportionality of any interference with those rights must be examined.²⁴⁵ In *Digital Rights Ireland*, the court invalidated the Data Retention Directive on the basis that it constituted a disproportionate interference with Articles 7,

²⁴² Treaty on European Union, art 6(1); Charter of Fundamental Rights of the European Union [2012] OJ C326/391.

²⁴³ Charter, art. 51(1).

²⁴⁴ Case C-571/10 *Servet Kamberaj v Istituto per l'Edilizia sociale della Provincia autonoma di Bolzano (IPES) and Others* [2012] ECLI:EU:C:2012:233, para 80; see also Case C-617/10 *Åkerberg Fransson* [2013] ECLI:EU:C:2013:105, paras 17-31.

²⁴⁵ Joined Cases C-92/09 and C-93/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen* [2010] ECLI:EU:C:2010:662, paras 47-50.

8, and 11 of the Charter.²⁴⁶ In *Schrems I* and *Schrems II*, the court invalidated decisions on the transfer of personal data to third countries on the basis of Charter-grounded analysis.²⁴⁷ In *La Quadrature du Net*, the court applied the same Charter-grounded methodology to national data retention regimes, holding that general and indiscriminate retention of traffic and location data is incompatible with Articles 7, 8, and 11 of the Charter.²⁴⁸

Article 1 of the Charter provides that "[h]uman dignity is inviolable. It must be respected and protected." The provision is foundational to the Charter as a whole, sitting in Title I (Dignity) and structurally preceding all other rights. The dual verbal formulation, requiring both respect and protection, has been read as imposing both negative and positive obligations on Union institutions and Member States.²⁴⁹ In the context of non-consensual deepfake pornography, Article 1 is engaged at the point at which a synthetic intimate representation of an identifiable woman is fabricated, regardless of whether the representation has been distributed or recognised by any particular viewer.

Article 3 provides that "[e]veryone has the right to respect for his or her physical and mental integrity." The provision extends beyond bodily integrity to encompass mental and psychological integrity.²⁵⁰ The harms documented in chapter 1, including the psychological dimensions of representational injury and the integrity-related dimensions of digital embodiment, fall within the scope of Article 3.

Article 7 provides that "[e]veryone has the right to respect for his or her private and family life, home and communications." The CJEU has interpreted Article 7 expansively in data protection contexts, treating interference with private life as engaged by the processing of personal data and assessing the gravity of any interference by reference to the nature and consequences of the processing and not just the data subject's awareness of it.²⁵¹ Article 7 corresponds to Article 8 of the European Convention on Human Rights and Article 52(3) of the Charter requires that Charter rights corresponding to ECHR rights have

²⁴⁶ Joined Cases C-293/12 and C-594/12 *Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014] ECLI:EU:C:2014:238, paras 33-37.

²⁴⁷ Case C-362/14 *Maximillian Schrems v Data Protection Commissioner* [2015] ECLI:EU:C:2015:650 (*Schrems I*); Case C-311/18 *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems* [2020] ECLI:EU:C:2020:559 (*Schrems II*).

²⁴⁸ Joined Cases C-511/18, C-512/18 and C-520/18 *La Quadrature du Net and Others v Premier ministre and Others* [2020] ECLI:EU:C:2020:791.

²⁴⁹ Charter, art 1; on Article 1 of the Charter and the dual-obligation structure of human dignity provisions, see Steve Peers, Tamara Hervey, Jeff Kenner and Angela Ward (eds), *The EU Charter of Fundamental Rights: A Commentary* (2nd edn, Hart 2021) ch 1.

²⁵⁰ Charter, art 3; on the mental and psychological dimensions of integrity under Article 3, see *Ibid.* ch 3.

²⁵¹ Volker und Markus Schecke paras 47-49; *Digital Rights Ireland* paras 33-37.

at least the same meaning and scope. The ECtHR has developed substantial jurisprudence on Article 8 ECHR in image-based abuse and online privacy contexts, which provides interpretive support for the reading of Article 7 advanced in section 5.2.²⁵²

Article 8 provides a freestanding right to the protection of personal data, distinct from the right to private life under Article 7. The provision sets out specific structural requirements for processing personal data: fairness, specified purpose, consent or another legitimate basis and the right of access and rectification. The CJEU has held that Article 8 confers an independent constitutional right whose protective scope cannot be narrowed by interpretive choices that exclude categories of harm the data protection framework was designed to address.²⁵³

Article 21 prohibits discrimination on any ground including sex. The provision works alongside Article 23, which requires that equality between women and men be ensured in all areas. These provisions provide the constitutional base for the substantive equality reading.²⁵⁴

Article 23 provides that "[e]quality between women and men must be ensured in all areas, including employment, work and pay." The CJEU and scholarly commentary have read Article 23 as requiring substantive equality.²⁵⁵ The substantive equality reading distinguishes between treating women and men identically regardless of differential outcomes (formal equality) and ensuring that legal frameworks do not produce systematic disadvantage to one sex relative to the other (substantive equality). In the context of GDPR interpretation, the substantive equality requirement has direct interpretive implications for provisions whose application produces gendered outcomes.

Article 52(1) of the Charter requires that any limitation on the exercise of Charter rights must be provided for by law, respect the essence of those rights, and be subject to the principle of proportionality, meaning that limitations may be made only if necessary and genuinely meet objectives of general interest recognised by the Union or the need to protect the rights and freedoms of others.²⁵⁶ This provision is the

²⁵² For ECtHR jurisprudence on Article 8 ECHR in image-based abuse and online privacy contexts, see *K.U. v Finland* App no 2872/02 (ECtHR, 2 December 2008); *M.L. and W.W. v Germany* App nos 60798/10 and 65599/10 (ECtHR, 28 June 2018); *Volodina v Russia* (No 2) App no 40419/19 (ECtHR, 14 September 2021).

²⁵³ *Volker und Markus Schecke* paras 47-49; Charter, art 8.

²⁵⁴ Charter, arts 21, 23.

²⁵⁵ Case C-407/98 *Abrahamsson and Anderson v Fogelqvist* [2000] ECLI:EU:C:2000:367, paras 47-48; Case C-450/93 *Kalanke v Freie Hansestadt Bremen* [1995] ECLI:EU:C:1995:322; Case C-409/95 *Marschall v Land Nordrhein-Westfalen* [1997] ECLI:EU:C:1997:533. See also Sandra Fredman, 'Substantive Equality Revisited' (2016) 14 *International Journal of Constitutional Law* 712.

²⁵⁶ Charter, art 52(1); on the proportionality test under Article 52(1), see *Schecke* (n 4) paras 50-52; *Digital Rights Ireland* paras 38-69.

structural mechanism through which Charter rights interact with each other and with other interests, including those protected by the GDPR's exceptions in Article 17(3). The proportionality framework provides the doctrinal vocabulary for assessing how the balancing exercises are structured. Based on that, it can be argued that any limitation on the rights of victims of non-consensual deepfake pornography under Articles 1, 3, 7, 8, and 23 must satisfy the proportionality test, including the requirements of necessity and respect for the essence of the rights at issue. That means that constitutional foundations outlined above require an interpretation of "personal data" under Article 4(1) GDPR and of "erasure" under Article 17 GDPR that the case law has not yet developed but that the textual provisions can sustain.

5.2 Reinterpreting "Personal Data"

Article 4(1) GDPR admits two readings. The narrow reading treats personal data as information from which the data subject can be recognised, making identifiability the gateway to protection. The broader reading, drawn from the result element of the Article 29 Working Party's tripartite 'relating to' test, treats information as personal data where its processing has direct consequences for the data subject's rights, regardless of identifiability. Chapter II established that both readings are textually available and that the broader reading better captures the harm at issue in non-consensual deepfake pornography. However, within the Charter framework, the broader reading is constitutionally required.

Article 1's requirement that human dignity be respected and protected has direct consequences for the scope of personal data.²⁵⁷ The harms documented in Chapter I, the dignitary violation that Nussbaum's framework characterises through all seven features of objectification, the representational injury that Öhman locates at the point of fabrication, do not depend on the victim being identifiable to any particular viewer.²⁵⁸ They are part of what fabricating a sexual representation of a real person does to that person, regardless of whether anyone has yet recognised her in the image. A definition of personal data that only protects the data subject once they have been identified is incompatible with Article 1's obligation to respect and protect human dignity.

²⁵⁷ Charter, art. 1.

²⁵⁸ Martha C Nussbaum, 'Objectification' (1995) 24 *Philosophy and Public Affairs* 249, 257; Carl Öhman, 'Introducing the Pervert's Dilemma: A Contribution to the Critique of Deepfake Pornography' (2020) 22 *Ethics and Information Technology* 133, 134.

Article 7's protection of private and family life, read in light of the digital embodiment framework introduced in section 1.4, requires that personal data extend to fabricated representations of the data subject's digital identity.²⁵⁹ If digital representations are extensions of embodied identity then a synthetic intimate image is information about the depicted person's private life. The CJEU has interpreted Article 7 expansively in data protection contexts, holding in *Volker und Markus Schecke* that interference with private life under Article 7 is engaged by any processing of personal data and that the gravity of the interference depends on the nature and consequences of the processing.²⁶⁰ The character of the synthetic image as information about private life remains true regardless of whether an observer without contextual knowledge can identify the data subject from it.

Article 8's freestanding protection of personal data was confirmed in *Volker und Markus Schecke*. Its consequence is that the regulation's protective scope cannot be narrowed through interpretive choices that exclude categories of harm the GDPR was designed to address.²⁶¹ The purposive principle articulated by the Working Party becomes, under Article 8, a Charter requirement.²⁶² Reading of Article 4(1) that excludes synthetic media on the basis that the output may not always satisfy the identifiability criterion does not align with the regulation's Charter-grounded purpose.

The Charter's binding force over the GDPR and the principle of consistent interpretation, both established in section 5.1, mean that Article 23's substantive equality requirement must inform the interpretation of GDPR provisions. As Chapter II established, the identifiability framework produces systematically weaker protection for private individuals than for publicly recognisable ones and offers protection only after identification not at the point of fabrication.²⁶³ In the deepfake context, where 96% of victims are women and where private individuals form an increasingly large share of those targeted, this pattern of protection is gendered in its outcomes.²⁶⁴ Article 23 requires that GDPR provisions be interpreted in a way that does not reproduce that pattern like Article 4(1) in its current reading does. The broader reading, which extends protection through the result element regardless of identifiability, does

²⁵⁹ Charter, art 7; N Katherine Hayles, *How We Became Posthuman: Virtual Bodies in Cybernetics, Literature, and Informatics* (University of Chicago Press 1999) 3.

²⁶⁰ Case C-92/09 *Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen* [2010] ECLI:EU:C: 2010:662, paras 47-49; C-594/12 *Digital Rights Ireland* [2014] ECLI:EU:C: 2014:238, paras 33-37.

²⁶¹ *Volker und Markus Schecke paras 47-48*; Charter, art 8.

²⁶² Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data (WP 136, 2007) 4.

²⁶³ Michelle Finck and Frank Pallas, 'They Who Must Not Be Identified: Distinguishing Personal from Non-Personal Data Under the GDPR' (2020) 10 *International Data Privacy Law* 11, 14.

²⁶⁴ Henry Ajder and others, *The State of Deepfakes: Landscape, Threats, and Impact* (Deeptrace 2019) https://regmedia.co.uk/2019/10/08/deepfake_report.pdf accessed 19 May 2026.

not. Weaker protection for individuals goes hand in hand with weaker protection for women, as it is women who make up the majority of victims of non-consensual deepfake pornography. A framework whose application produces this outcome cannot be reconciled with the substantive equality requirement Article 23 imposes, particularly when an alternative interpretation that does not produce that outcome is textually available.

The result element of the tripartite "relating to" test must function as a primary rather basis for personal data status. Where processing has direct and serious consequences for the rights of an identifiable person, those consequences themselves are enough to establish that the information relates to her within the meaning of Article 4(1).²⁶⁵ The Working Party's caution against overstretching the definition does not bear on cases where the consequences are certain, severe and traceable, as they are in non-consensual deepfake pornography.²⁶⁶ The identifiability standard in Recital 26 must be applied with a dynamic understanding of the means available to identify individuals. The reasonable likelihood criterion already permits this.²⁶⁷ Facial recognition technology, reverse image search tools and biometric matching systems make identification reasonably possible for a substantially wider category of individuals than the framework's traditional application has supposed. The standard needs to be applied in a way that reflects this. The protection of biometric data under Article 9 works independently of the output question. The processing of biometric input data extracted from publicly available images, for the purpose of generating synthetic intimate content, is unlawful processing of special category personal data regardless of how the output is characterised.²⁶⁸ Supervisory authorities and controllers should treat Article 9 as the part of the GDPR's coverage in the deepfake context and it should not be open to dispute.

These consequences make the GDPR's framework available to victims of non-consensual deepfake pornography as a matter of legal entitlement. The right to erasure can be invoked on the broader basis the Charter requires. The procedural pathways the Article 17 framework provides become accessible to victims who would otherwise be excluded from them.

²⁶⁵ Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data (WP 136, 2007) 10–11; Case C-434/16 Peter Nowak v Data Protection Commissioner [2017] ECLI:EU:C:2017:994, paras 34–35.

²⁶⁶ Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data (WP 136, 2007) 5.

²⁶⁷ GDPR, Recital 26; Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland [2016] ECLI:EU:C:2016:779, para 46.

²⁶⁸ GDPR, arts 4(14), 9(1), 9(2).

5.3 Reinterpreting "Erasure"

Article 17 GDPR sets out a right to erasure but does not define erasure with precision. The text obliges the controller to erase personal data "without undue delay" where one of the grounds in Article 17(1) is engaged.²⁶⁹ Article 17(2) requires controllers who have made personal data public to take "reasonable steps" to inform other controllers processing the data of the data subject's request.²⁷⁰ Both formulations, similarly to the "personal data", admit two readings. The narrow reading treats erasure as deletion at source, meaning the controller removes data from its own records and is obligated to notify other controllers. The broader reading understands erasure as effective removal from circulation. That means that under Article 17(2) the controller's obligation is to be discharged in a manner that delivers the protection of the data subject from continued exposure to the harm the data causes. Again, as with the "personal data" issue, both readings are textually available, but only the broader one falls within the Charter's framework.

Crucial provisions of the Charter in this case are the ones dealing with dignity and integrity. In the deepfake context, the harms that erasure under Article 17 GDPR is meant to address, engage dignity directly.²⁷¹ Removal of content from one controller's records, while it still circulates across other easily accessible platforms only relocates data subject's exposure to that harm. Argument here can be extended to the Article 3's protection of mental and psychological integrity. If it is the continued availability of the content that produces the harm to integrity, then removal that does not address availability does not provide the protection the law is intended to ensure. The Charter does not require erasure to be perfect, but it does require erasure to be effective.

The CJEU's existing case law has already taken steps toward this reading, although not in cases involving the harms central to this thesis. In *Google Spain*, the court held that erasure includes the de-referencing of links to underlying content by search engines, recognising that the controller's obligation extends beyond its own data holdings to the role it plays in making content discoverable.²⁷² In *TU and RE v Google*, this reasoning was extended and a separate balancing exercise was introduced.²⁷³ Both cases recognise that the data subject's interest in erasure cannot be limited to deletion at source. The

²⁶⁹ *ibid* Art. 17(2)

²⁷⁰ *ibid* Art. 17(2)

²⁷¹ Charter, arts 1,3.

²⁷² *Google Spain* paras 80-88.

²⁷³ *Tu and RE v Google LLC*, paras 95-108.

foundation set out in section 5.1 supports extending this trajectory further. Where the content is non-consensual synthetic intimate imagery, the right to erasure must reach the platforms and search results where the harm is being done. Reading the right this way also affects how the balancing exercise critiqued in chapter 4 should operate. Section 4.3 showed that the framework treats deepfake content as expressive material whose removal requires justification against Article 11 expression interests. The Charter foundation supports reframing that analytical position. Where the content fails to engage Article 11 in any substantive sense, the framework's presumption that removal must be justified against expressive interests does not apply with the force the existing case law assigns to it. *TU and RE v Google* itself supports this. The Court held that where the data subject submits relevant and sufficient evidence establishing the manifest inaccuracy of information, the search engine must accede to the request and the right to freedom of expression "cannot include the right to disseminate and have access to such information."²⁷⁴ Non-consensual deepfake pornography is essentially fabricated content depicting events that never took place while showcasing people that never consented to it. The expressive interest in disseminating such content does not withstand Article 52(1)'s requirement that limitations on Charter rights respect the essence of those rights.²⁷⁵ The dignity, integrity and substantive equality interests of the data subject must take precedence over "expressive" interest in such scenarios.

The temporal dimension of the right also follows from this reading. Article 17(1) requires erasure "without undue delay".²⁷⁶ The phrase has been read in practice as a procedural standard for the controller's response time. The Charters foundation, however, supports reading it more substantively. Where the harm escalates with each viewing, each share, each download, the constitutional function of the right requires that erasure arrive before the harm becomes effectively irreversible. The reasonable-steps obligation under Article 17(2), read against the Charter foundation, should be understood to include the obligation to act with the urgency the harm requires.²⁷⁷

The right to be forgotten should be understood to require effective removal from circulation rather than only deletion at source. Substantive duty should be imposed on the controllers with Article 17(2) being the source of this obligation. The balancing exercise within Article 17(3)(a) should proceed from an analytical position that does not presume expressive value where the content fails to engage Article 11 in substance. The "without undue delay" requirement should be read as carrying the temporal urgency

²⁷⁴ Ibid para 65.

²⁷⁵ Charter, art 52(1).

²⁷⁶ GDPR, art17(1).

²⁷⁷ ibid art 17(2)

the harm requires. None of these readings creates a new right that the GDPR does not already contain. Each reads existing textual provisions in light of the Charter.

5.4 The Limits of Reinterpretation

The reinterpretation developed in sections 5.2 and 5.3 makes the GDPR substantially more available to victims of non-consensual deepfake pornography than the case law currently suggests. However, it is not an unflawed solution.

The first issue worth addressing is the territorial scope of the GDPR. As any EU law, its territorial jurisdiction is the Union's territory. Under Article 3 GDPR, it applies to controllers and processors established in the Union and to those established outside the Union where they offer goods or services to data subjects in the Union or monitor their behaviour within the Union.²⁷⁸ However broad it may seem, it is not unlimited. Many platforms that host deepfake content, especially those ones hosting non-consensual intimate imagery, operate from jurisdictions that fall outside the GDPR's reach.²⁷⁹ The EDPB's guidance on territorial scope confirms that intentional targeting of EU data subjects is what triggers Article 3(2) application.²⁸⁰ Processing that does not target EU users does not fall within the GDPR even when EU residents access the platform.²⁸¹ Reinterpretation of Articles 4(1) and 17 does not extend the territorial reach of the regulation, therefore what does not fall within the GDPR's scope cannot be addressed by reinterpreting the GDPR's provisions.

Another issue is the enforcement capacity. Such a reinterpretation will not be possible unless the supervisory authorities and the national courts adopt a broader interpretation of the provisions in question. Even where the constitutional foundation supports the broader readings, supervisory authorities operate with limited resources, significant complaint backlogs and varying institutional cultures across Member States.²⁸² A right that is theoretically available to victims is not the same as a right that is

²⁷⁸ *ibid* art 3.

²⁷⁹ On platforms specifically created to host non-consensual intimate imagery and the jurisdictional challenges they present, see Henry Ajder and others, *The State of Deepfakes: Landscape, Threats, and Impact* (Deeptrace 2019) ; Danielle Keats Citron, 'Sexual Privacy' (2019) 128 *Yale Law Journal* 1870, 1909-1915.

²⁸⁰ European Data Protection Board, *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)* (Version 2.1, 12 November 2019) 12-14.

²⁸¹ *ibid*

²⁸² Orla Lynskey, 'The "Europeanisation" of Data Protection Law' (2017) 19 *Cambridge Yearbook of European Legal Studies* 252, 273-280; European Parliament, *Resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application (2020/2717(RSP))* paras 15-20.

practically accessible. Reinterpretation alone cannot create the enforcement capacity that effective implementation requires.

Structural limits must also be addressed. The right to be forgotten works only against the controller responsible for the processing of the personal data and not against the creator of the synthetic content.²⁸³ GDPR's architecture allows only for an intervention once the content has already been shared and is being processed by a controller. It is not possible for it to deal with the harm caused just with the creation of the deepfake. Even the best reinterpretation cannot change that. Where the harm originates with creators operating outside the regulation's controller-processor framework, the right to erasure has nothing to say.

Next problem at hand is the remedial value of the solution. Erasure deals with removal of data and does not produce compensation for harm already inflicted, criminal sanctions against perpetrators, or restoration of dignity in any deep sense. The Charter foundation supports reading the right to deliver effective removal, but effective removal is not effective remedy. Where dignity and reputation have already been harmed by content's circulation, removal will not remedy the damage caused. The reinterpretation cannot transform a removal right into a comprehensive remedial regime.²⁸⁴

The final limit is the limit of interpretation as a methodology itself. The CJEU has consistently held that the principle of consistent interpretation cannot require *contra legem* readings of national or EU law.²⁸⁵ Interpretation works within the textual provisions of the GDPR and reads them in light of the Charter. No new laws may be established that have not been enacted by the legislature, nor may the restrictions arising from the wording of the provisions being interpreted be disregarded. The reinterpretation in 5.2 and 5.3 works because the textual provisions can sustain the broader readings. Other solutions that depend on importing concepts that GDPR does not contain, would require legislative action.²⁸⁶

²⁸³ GDPR art. 4(7); GDPR art. 17(1).

²⁸⁴ Clare McGlynn and Erika Rackley, 'Image-Based Sexual Abuse' (2017) 37 *Oxford Journal of Legal Studies* 534, 553-558.

²⁸⁵ Case C-212/04 *Adeneler and Others v Ellinikos Organismos Galaktos* (ELOG) [2006] ECLI:EU:C:2006:443, para 110; Case C-441/14 *Dansk Industri (DI) v Estate of Karsten Eigil Rasmussen* [2016] ECLI:EU:C:2016:278, paras 32-33; Case C-105/03 *Pupino* [2005] ECLI:EU:C:2005:386, para 47.

²⁸⁶ Koen Lenaerts and José Antonio Gutiérrez-Fons, 'To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice' (2013) 20 *Columbia Journal of European Law* 3, 49-53.

These limits are broad and that is why the GDPR is best understood as one component of a complex EU legal response to a complex issue that deepfake pornography is.²⁸⁷ GDPR can be one part of the solution.²⁸⁸ The AI Act, which entered into force in August 2024, addresses synthetic content directly.²⁸⁹ Article 50(4) imposes transparency obligations on deployers of AI systems that generate deepfakes, requiring disclosure that the content has been artificially generated or manipulated.²⁹⁰ Article 50(2) requires providers of generative AI systems to mark outputs in a machine-readable format and ensure detectability.²⁹¹ These provisions operate on the production and distribution side that the GDPR's controller-processor architecture cannot reach. The Digital Services Act adds a content-moderation framework on platforms regardless of whether they qualify as data controllers under the GDPR.²⁹² Criminal law in Member States starts to acknowledge the issue and address the production and dissemination of non-consensual intimate imagery directly.²⁹³ However, none of these elements alone is sufficient for dealing with this highly complex issue. Together, they form an interconnected regulatory architecture in which each instrument addresses what the others cannot.

5.5 Practical Implications and Improvements Stemming from Feminist Reinterpretation

The reinterpretation presented in the previous sections produced specific consequences for how the GDPR functions in cases involving non-consensual pornography. These consequences stem from the constitutional requirement that the provisions of the GDPR must be interpreted in a way that does not reproduce the gendered pattern of weaker protection. Article 23 of Charter, together with Article 1 and 3, makes these consequences obligatory.²⁹⁴

²⁸⁷ M. Łabuz “Regulating Deep Fakes in the Artificial Intelligence Act,” ACIG, vol. 2, no. 1, 2023, DOI: 10.60097/ACIG/162856, 26-30.

²⁸⁸ *ibid*

²⁸⁹ Regulation (EU) 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 L, 2024/1689; the regulation entered into force on 1 August 2024.

²⁹⁰ *ibid* art 50(4)

²⁹¹ *ibid* art 50(2)

²⁹² 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) [2022] OJ L277/1.

²⁹³ For comparative analysis of Member State criminal law approaches to non-consensual deepfake pornography, see Karolina Mania, 'Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings From a Comparative Legal Study' (2024) 25 *Trauma, Violence, & Abuse* 117.

²⁹⁴ Charter, arts 1, 3, 23.

The most concrete site of operational change is the work of national data protection authorities and the EDPB. Supervisory authorities make daily decisions about how the GDPR's provisions apply and the reinterpretation directly affects those decisions. In February 2026, the EDPB published its Coordinated Enforcement Framework report on Article 17, identifying seven systemic weaknesses in how controllers implement the right to erasure across Member States.²⁹⁵ The report confirms that the law on paper is not the same as the law in practice.²⁹⁶ The gap between formal availability and practical accessibility is the gap the substantive equality requirement under Article 23 is designed to address.

In accordance with the reinterpretation, supervisory authorities must meet new requirements. They should treat synthetic content depicting an identifiable woman as personal data within the meaning of Article 4(1), even where the output may not satisfy traditional identifiability tests at the moment of fabrication.²⁹⁷ The result element of the tripartite "relating to" test can provide the doctrinal basis for this treatment. Supervisory authorities should treat biometric input data extracted from publicly available images for the purpose of generating synthetic intimate content as unlawful processing of special category personal data under Article 9. This point should be beyond dispute, even if the definitional issues surrounding output remain unresolved. Supervisory authorities should recognise the temporal dimension of erasure that section 5.3 developed. The removal of content after it has been widely disseminated protects something other than Articles 1 and 3 aim to protect.

The EDPB has a particular institutional role here. The Coordinated Enforcement Framework provides a mechanism through which the reinterpretation can be operationalised across Member States, addressing the institutional-culture variation 5.4 identified as a limit.²⁹⁸ If the feminist reinterpretation presented in the previous chapters were to be read in conjunction with the EDPB report, it would evolve from a doctrinal argument into supervisory practice. The CEF report's identification of "inadequate internal procedures" and "insufficient information provided to data subjects" as systemic weaknesses indicates that such guidance is institutionally needed.²⁹⁹

The reinterpretation has direct consequences for how platforms process erasure requests. As previously established, non-consensual deepfake porn has no expressive value. Therefore, platforms

²⁹⁵ European Data Protection Board, 2025 Coordinated Enforcement Action: Implementation of the right to erasure by controllers (Adopted 17 February 2026) ('CEF 2025 Report').

²⁹⁶ *ibid*

²⁹⁷ GDPR art. 4(1).

²⁹⁸ European Data Protection Board, 2025 Coordinated Enforcement Action: Implementation of the right to erasure by controllers (Adopted 17 February 2026) ('CEF 2025 Report') section 3.

²⁹⁹ *ibid* sections 4.2.3. and 4.2.4

acting as controllers cannot treat erasure requests concerning such content as ordinary content disputes to be processed within standard turnaround times, are wrong. The requests engage Article 1 and Article 3 of the Charter from the moment they are received, which has implications for both the response time and the substantive analysis that platforms must apply.

The Article 17(2) obligation to take reasonable steps to inform other controllers should operate substantively. Where the same content circulates across platforms, the original controller's obligation is not discharged by deletion of its own records alone. The requirement of substantive equality under Article 23, which reinforces the procedural interpretation of Article 17(2), reflects the pattern of reduced protection identified in section 5.2, as it is women, whose images circulate across multiple platforms, who bear the practical burden of pursuing claims against each data controller individually. The Charter foundation does not permit this allocation of burden.

For courts and supervisory authorities adjudicating Article 17 disputes, the reinterpretation provides a Charter-grounded analytical position from which the balancing exercise should be conducted. The assumption that content falling within the scope of Article 17(3)(a) has expressive value cannot apply in the same way where that content consists of synthetically generated intimate images depicting an identifiable woman without her consent. It does not sustain Article 52(1)'s requirement that limitations on Charter rights respect the essence of those rights. The dignity, integrity and substantive equality interests of the data subject must take precedence over the "expressive" interest in such scenarios. This is a recommendation to conduct the balance from the analytical position the Charter foundation requires.

For victims and their advocates, the reinterpretation makes the GDPR meaningfully available as a remedial pathway. Claims under Article 17 can be advanced on the Charter-grounded basis the chapter has developed, as claims engaging dignity, integrity and substantive equality. It shifts the analytical position from which advocacy proceeds. A claim framed as one of identifiability invites the controller and, on appeal, the supervisory authority to test the claim against the narrow reading of Article 4(1). A claim framed as one of dignity, integrity and substantive equality invites the same actors to engage with the Charter foundation. The doctrinal terrain on which the claim is contested is different and the difference matters for the claim's prospects of success. The reinterpretation of Article 17 mean that the GDPR can carry analytical weight that the current case law has not yet assigned to it. This matters for how advocates situate the GDPR claim within the broader response to the harm. Where a victim is pursuing criminal proceedings against an identified perpetrator, the GDPR claim runs alongside the criminal case as a removal-focused remedy that does not depend on identification of the creator. Where

the perpetrator is unknown or operates from a jurisdiction that does not address the conduct, the GDPR claim against the platform may be the only available route to removal. Where the platform itself is uncooperative, supervisory authority enforcement and, ultimately, judicial enforcement can operate as a structured escalation pathway. Advocates working with victims should also be aware of the temporal dimension the reinterpretation surfaces. They could press supervisory authorities to treat delays in platform response as themselves potential violations of Article 17, distinct from refusals to comply altogether.

The practical implications set out above should be understood within the broader EU regulatory architecture. The AI Act's Article 50 transparency obligations operate on the production side of synthetic content. The DSA's content-moderation framework oversees platforms regardless of their controller status. Member State criminal law on non-consensual intimate imagery addresses the perpetrators directly. The reinterpreted GDPR sits within this architecture as the instrument that gives victims a Charter-grounded right of removal available to them as a matter of legal entitlement. None of these instruments alone is sufficient to address the harm. Together they form a layered legal response that is adequate to the gendered structure of the harm. What the feminist reinterpretation contributes to that architecture is the recognition that the GDPR was never gender-neutral in its operation and that its proper interpretation requires it to stop functioning as if it were. Whether we decided to acknowledge that or not means that “freedom of women from sex oppression either matters or it does not; it is either essential or it is not. Decide one more time.”³⁰⁰

³⁰⁰ Andrea Dworkin, *Right-Wing Women* (Perigee Books 1983), 227.

Conclusion

This thesis began with a question about whether the failure of EU law to remedy non-consensual deepfake pornography is structural and whether it can be addressed through reinterpretation of existing provisions. The answer that has emerged across the preceding chapters is that the failure is structural, that the structure can be identified and named and that the right to erasure under Article 17 GDPR can be made to do work the current case law has not assigned to it. The reinterpretation that delivers this work is what the Charter of Fundamental Rights requires.

Presented argument rests firstly on the fact that the harm of non-consensual deepfake pornography is a gendered, structural harm. 96% of deepfake videos online depict women without their consent. The harm caused engages dignity, integrity and substantive equality in ways that doctrinal analysis blind to these dimensions cannot register. Another present issue is that the GDPR's foundational concepts admit broader readings than the case law has so far developed. Personal data under Article 4(1) can be read through the result element of the tripartite "relating to" test to capture synthetic content depicting an identifiable person regardless of whether the output satisfies traditional identifiability standards. Erasure under Article 17 can be read substantively, requiring effective removal from circulation. Finally, these broader readings are required by Articles 1, 3, 7, 8 and 23 of the Charter read together and by the principle of consistent interpretation that obliges EU secondary legislation to be read in conformity with the Charter wherever the text permits.

What the thesis has contributed is a sustained Charter-grounded feminist reinterpretation of EU data protection law in the deepfake context. Existing doctrinal literature on Article 17 has not engaged with the gendered structure of the harm. The feminist literature on image-based abuse has engaged primarily with US law and has not been systematically applied to EU data protection doctrine. By bringing MacKinnon's structural critique, Citron's framework of sexual privacy and Öhman's concept of representational injury into sustained engagement with the CJEU's case law on personal data and erasure, the connection between the two systems is being made. The thesis identifies where the existing framework fails women and what doctrinal resources are available within the framework to address that failure. The systematic critique of the balancing framework under Article 17(3)(a) as structurally biased, developed in chapter 4, is also a contribution. The framework's presumption of expressive value, its treatment of public interest and its role-in-public-life factor were all developed in cases that did not and

could not have involved the harm at issue and the thesis identifies the consequences of that structural mismatch.

The work has limits. It is doctrinal rather than empirical and it does not engage with how victims experience GDPR enforcement, how supervisory authorities decide deepfake-related complaints or how platforms respond to erasure requests in this context. These are questions for empirical scholarship that this thesis cannot answer. The argument also depends on case law that has not yet addressed non-consensual deepfake pornography directly. National courts have not referred Article 17 preliminary questions involving synthetic intimate imagery and the doctrinal landscape may shift as such cases arrive. The reinterpretation developed here is the reading the Charter requires, but its institutional uptake by supervisory authorities, national courts and ultimately the CJEU remains a question that only time and litigation will resolve. The thesis also stays within the scope of EU law. Comparative analysis with other regimes that have addressed deepfake harm, particularly the UK's Online Safety Act and the US Take It Down Act would deepen the picture this work begins to draw.

Further work suggests itself in several directions. Empirical research on how victims engage with EU data protection authorities in deepfake cases would test the practical accessibility of the reinterpretation argued for here. Comparative analysis of how the GDPR, AI Act and DSA interact in practice as platforms implement the new transparency and content-moderation requirements would clarify where the integrated regulatory architecture works and where it fails. Deeper engagement with intersectional analysis, particularly the differential experience of women of colour, trans women, and non-binary individuals who appear in the empirical literature as bearing compounded harm, would extend the feminist analytical work the thesis begins.

What the thesis has tried to show is that the GDPR was never gender-neutral in its operation. It has produced gendered outcomes because it has been interpreted within a framework that treated identifiability and expressive value as neutral analytical categories when they were, in fact, calibrated to harms whose primary victims were not women. The Charter exists, in part, to prevent EU law from operating in this way. Reading the GDPR through the Charter is what the existing legal framework requires. The thesis proves that broad reading of GDPR must be treated as constitutionally available. Whether that move is taken up by supervisory authorities and courts is a question that will be answered, one case at a time, by the institutions that decide whether the harm being done to women in the digital environment matters enough to be recognised by the legal frameworks that purport to address it.

Bibliography:

Book and Monographs

1. Citron DK, Hate Crimes in Cyberspace (Harvard University Press 2014).
2. Citron DK, The Fight for Privacy: Protecting Dignity, Identity, and Love in the Digital Age (W W Norton 2022).
3. Cohen JE, Between Truth and Power: The Legal Constructions of Informational Capitalism (Oxford University Press 2019).
4. Dworkin A, Right-Wing Women (Perigee Books 1983).
5. Hayles NK, How We Became Posthuman: Virtual Bodies in Cybernetics, Literature, and Informatics (University of Chicago Press 1999).
6. Hildebrandt M, Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology (Edward Elgar 2015).
7. Kant I, Groundwork of the Metaphysics of Morals (Mary Gregor tr, Cambridge University Press 1998).
8. Karolina Mania, 'Legal Protection of Revenge and Deepfake Porn Victims in the European Union' (2024) 25 Trauma, Violence, & Abuse 117.
9. Lessig L, Code: Version 2.0 (Basic Books 2006).
10. Lynskey O, The Foundations of EU Data Protection Law (Oxford University Press 2015).
11. MacKinnon, Feminism Unmodified: Discourses on Life and Law (Harvard University Press 1987).
12. MacKinnon CA, Only Words (Harvard University Press 1993).
13. MacKinnon CA, Toward a Feminist Theory of the State (Harvard University Press 1989).
14. Nussbaum MC, Hiding from Humanity: Disgust, Shame, and the Law (Princeton University Press 2004).
15. Nussbaum MC, Sex and Social Justice (Oxford University Press 1999).
16. Peers S, Hervey T, Kenner J and Ward A (eds), The EU Charter of Fundamental Rights: A Commentary (2nd edn, Hart 2021).
17. Richards NM, Intellectual Privacy: Civil Liberties and Information in the Digital Age (Oxford University Press 2015).
18. Schauer F, Free Speech: A Philosophical Enquiry (Cambridge University Press 1982).
19. Smart C, Feminism and the Power of Law (Routledge 1989).

20. Waldron J, *Dignity, Rank, and Rights* (Oxford University Press 2012).

Journal Articles

1. Alanazi S and Asif S, 'Exploring Deepfake Technology: Creation, Consequences and Countermeasures' (2024) 6 *Human-Intelligent Systems Integration* 49.
2. Ausloos J, 'The "Right to Be Forgotten" - Worth Remembering?' (2012) 28 *Computer Law and Security Review* 143.
3. Bartlett KT, 'Feminist Legal Methods' (1990) 103 *Harvard Law Review* 829.
4. Bates S, 'Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors' (2017) 12 *Feminist Criminology* 22.
5. Chesney R and Citron DK, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 *California Law Review* 1753.
6. Citron DK and Norton H, 'Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age' (2011) 91 *Boston University Law Review* 1435.
7. Citron DK, 'Sexual Privacy' (2019) 128 *Yale Law Journal* 1870.
8. Cohen JE, 'What Privacy Is For' 126 *Harvard Law Review* 1904 (2013).
9. Crenshaw K, 'Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics' (1989) *University of Chicago Legal Forum* 139.
10. Crenshaw K, 'Mapping the Margins: Intersectionality, Identity Politics, and Violence Against Women of Color' (1991) 43 *Stanford Law Review* 1241.
11. De Silva De Alwis R and Carey P, 'A Rapidly Shifting Landscape: Why Digitized Violence is the Newest Category of Gender-Based Violence' (2023) *Public Law and Legal Theory Research Paper Series*, Research Paper No 23.
12. Delfino RA, 'Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act' (2019) 88 *Fordham Law Review* 887.
13. Finck M and Pallas F, 'They Who Must Not Be Identified: Distinguishing Personal from Non-Personal Data Under the GDPR' (2020) 10 *International Data Privacy Law* 11.
14. Franks MA, 'Unwilling Avatars: Idealism and Discrimination in Cyberspace' (2011) 20 *Columbia Journal of Gender and Law* 224.
15. Fredman S, 'Substantive Equality Revisited' (2016) 14 *International Journal of Constitutional Law* 712.

16. Goodfellow IJ and others, 'Generative Adversarial Nets' (Neural Information Processing Systems Conference Paper, 10 June 2014).
17. Harris D, 'Deepfakes: False Pornography is Here and the Law Cannot Protect You' (2019) 17 Duke Law and Technology Review 99.
18. Henry N and Powell A, 'Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law' (2016) 25 Social & Legal Studies 397.
19. Henry N and others, Image-Based Sexual Abuse: A Study on the Causes and Consequences of Non-Consensual Nude or Sexual Images (RMIT University 2019).
20. Karras T and others, 'Progressive Growing of GANs for Improved Quality, Stability, and Variation' (ICLR Conference Paper, April 2018) http://research.nvidia.com/sites/default/files/pubs/2017-10_Progressive-Growing-of/karras2018iclr-paper.pdf accessed 10 April 2026.
21. Kuczerawy A and Ausloos J, 'From Notice-and-Takedown to Notice-and-Delist: Implementing Google Spain' (2016) 14 Colorado Technology Law Journal 219.
22. Łabuz M, 'Regulating Deep Fakes in the Artificial Intelligence Act' (2023) 2(1) Applied Cybersecurity & Internet Governance, DOI: 10.60097/ACIG/162856.
23. Lenaerts K and Gutiérrez-Fons JA, 'To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice' (2013) 20 Columbia Journal of European Law 3.
24. Lynskey O, 'The "Europeanisation" of Data Protection Law' (2017) 19 Cambridge Yearbook of European Legal Studies 252.
25. McGlynn C and Rackley E, 'Image-Based Sexual Abuse' (2017) 37 Oxford Journal of Legal Studies 534.
26. McGlynn C, Rackley E and Houghton R, 'Beyond "Revenge Porn": The Continuum of Image-Based Sexual Abuse' (2017) 25 Feminist Legal Studies 25.
27. Nussbaum MC, 'Objectification' (1995) 24 Philosophy and Public Affairs 249.
28. Öhman C, 'Introducing the Pervert's Dilemma: A Contribution to the Critique of Deepfake Pornography' (2020) 22 Ethics and Information Technology 133.
29. Powell A and Henry N, 'Technology-Facilitated Sexual Violence Victimization: Results from an Online Survey of Australian Adults' (2019) 34 Journal of Interpersonal Violence 3637.
30. Suwajanakorn S and others, 'Synthesizing Obama: Learning Lip Sync from Audio' (2017) 36 ACM Transactions on Graphics, art 95

http://grail.cs.washington.edu/projects/AudioToObama/siggraph17_obama.pdf accessed 10 April 2026.

Reports and Policy Documents

1. Ajder H and others, The State of Deepfakes: Landscape, Threats, and Impact (Deeprace 2019) https://regmedia.co.uk/2019/10/08/deepfake_report.pdf accessed 11 April 2026.
2. Article 29 Data Protection Working Party, Opinion 4/2007 on the Concept of Personal Data (WP 136, 2007) <https://www.pdp.ie/docs/1030.pdf> accessed 16 April 2026.
3. Article 29 Working Party, Opinion 3/2012 on Developments in Biometric Technologies (WP 193).
4. Cavalli F and others, The State of Deepfakes 2024 (Sensity AI 2024) <https://5865987.fs1.hubspotusercontent-na1.net/hubfs/5865987/SODF%202024.pdf> accessed 11 April 2026.
5. Cyber Civil Rights Initiative, End Revenge Porn: A Survey of Victims (CCRI 2014) <https://cybercivilrights.org> accessed 11 April 2026.
6. EDPB, 2025 Coordinated Enforcement Action: Implementation of the Right to Erasure by Controllers.
7. European Data Protection Board, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) (Version 2.1, 12 November 2019).
8. European Data Protection Board, Guidelines 5/2019 on the Criteria of the Right to Be Forgotten in the Search Engines Cases Under the GDPR (2020).
9. European Parliament, Combating Gender-Based Violence: Cyber Violence (PE 662.621, 2021).
10. European Parliament, Resolution of 25 March 2021 on the Commission evaluation report on the implementation of the General Data Protection Regulation two years after its application (2020/2717(RSP)).
11. Europol, Facing Reality? Law Enforcement and the Challenge of Deepfakes (Europol Innovation Lab 2022).
12. Law Commission, Intimate Image Abuse: A Final Report (Law Com No 407, 2022).
13. 'European Court of Justice Limits the Territorial Scope of the "Right to Be Forgotten"' (European Parliamentary Research Service, PE 642.273, October 2019)

- [https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/642273/EPRS_ATA\(2019\)642273_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/ATAG/2019/642273/EPRS_ATA(2019)642273_EN.pdf) accessed 29 April 2026.
14. Security Hero, 2023 State of Deepfakes: Realities, Threats, and Impact (Security Hero 2023) <https://www.securityhero.io/state-of-deepfakes/> accessed 22 April 2026
15. UN Special Rapporteur on Violence Against Women, Online Violence Against Women and Girls: A Form of Gender-Based Discrimination (A/HRC/38/47, 2018).

Online Sources

1. 'Katie Hill: When a Politician's Nude Photos Are Leaked' (BBC, 2019) <https://www.bbc.com/audio/play/w3cszc27> accessed 12 April 2026
2. Khalili M, 'Deepfake Statistics 2025: AI Fraud Data and Trends' (Deepstrike, 8 September 2025) <https://deepstrike.io/blog/deepfake-statistics-2025> accessed 11 April 2026
3. Knight W, 'Real or Fake? AI is Making it Very Hard to Know' (MIT Technology Review, 1 May 2017) <https://www.technologyreview.com/s/604270/real-or-fake-ai-is-making-it-very-hard-to-know> accessed 10 April 2026
4. Somers M, 'Deepfakes, explained' (MIT Sloan Management Review, 21 July 2020) <https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained> accessed 10 April 2026

Case Law

1. Case C-101/01 Bodil Lindqvist [2003] ECLI:EU:C:2003:596
2. Case C-105/03 Pupino [2005] ECLI:EU:C:2005:386.
3. Case C-131/12 Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González [2014] ECLI:EU:C:2014:317.
4. Case C-136/17 GC and Others v Commission nationale de l'informatique et des libertés (CNIL) [2019] ECLI:EU:C:2019:773.
5. Case C-212/04 Adeneler and Others v Ellinikos Organismos Galaktos (ELOG) [2006] ECLI:EU:C:2006:443.
6. Case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems [2020] ECLI:EU:C:2020:559.
7. Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015] ECLI:EU:C:2015:650.

8. Case C-407/98 Abrahamsson and Anderson v Fogelqvist [2000] ECLI:EU:C:2000:367.
9. Case C-409/95 Marschall v Land Nordrhein-Westfalen [1997] ECLI:EU:C:1997:533.
10. Case C-434/16 Peter Nowak v Data Protection Commissioner [2017] ECLI:EU:C:2017:994
11. Case C-441/14 Dansk Industri (DI) v Estate of Karsten Eigil Rasmussen [2016] ECLI:EU:C:2016:278.
12. Case C-450/93 Kalanke v Freie Hansestadt Bremen [1995] ECLI:EU:C:1995:322.
13. Case C-460/20 TU and RE v Google LLC [2022] ECLI:EU:C:2022:962.
14. Case C-507/17 Google LLC v Commission nationale de l'informatique et des libertés (CNIL) [2019] ECLI:EU:C:2019:772.
15. Case C-571/10 Servet Kamberaj v Istituto per l'Edilizia sociale della Provincia autonoma di Bolzano (IPES) and Others [2012] ECLI:EU:C:2012:233.
16. Case C-582/14 Patrick Breyer v Bundesrepublik Deutschland [2016] ECLI:EU:C:2016:779.
17. Case C-617/10 Åkerberg Fransson [2013] ECLI:EU:C:2013:105.
18. Joined Cases C-293/12 and C-594/12 Digital Rights Ireland Ltd v Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others [2014] ECLI:EU:C:2014:238.
19. Joined Cases C-511/18, C-512/18 and C-520/18 La Quadrature du Net and Others v Premier ministre and Others [2020] ECLI:EU:C:2020:791.
20. Joined Cases C-92/09 and C-93/09 Volker und Markus Schecke GbR and Hartmut Eifert v Land Hessen [2010] ECLI:EU:C:2010:662.
21. K.U. v Finland App no 2872/02 (ECtHR, 2 December 2008).
22. M.L. and W.W. v Germany App no 60798/10 and 65599/10 (ECtHR, 28 June 2018).
23. Volodina v Russia (No 2) App no 40419/19 (ECtHR, 14 September 2021).

Legal Acts

1. Charter of Fundamental Rights of the European Union [2012] OJ C326/391.
2. Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, as amended) (ECHR).
3. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.
4. Online Safety Act 2023 (UK).

5. 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) [2016] OJ L119/1.
6. 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) [2022] OJ L277/1.
7. Regulation (EU) 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 L, 2024/1689.
8. Treaty on European Union [2012] OJ C326/13.