



A EUROPEAN CRIMINAL LAW APPROACH TO DEEPFAKE PORNOGRAPHY

Master Thesis LL.M. – Law and Technology

Student: Paolo Belloni
31/5/2024

First Supervisor: Pratham Ajmera
Second Supervisor: Gert Meyers

Table of Contents:

CHAPTER 1 - INTRODUCTION	1
1.1 Background.....	1
1.2 Problem statement	3
1.3 Research question and sub-questions.....	4
1.4 Literature review	4
1.5 Methodology and overview of the chapters	7
CHAPTER 2 - NOTION AND FEATURES OF DEEPPAKE PORNOGRAPHY	8
2.1 Introduction	8
2.2 Deepfake pornography as the misuse of a technology	8
2.3 Deepfake pornography as a social phenomenon.....	9
2.4 The distribution, creation, and possession of deepfake pornography as morally objectionable behaviors	10
2.5 Final remarks	12
CHAPTER 3 - A COMPARATIVE PERSPECTIVE ON CURRENT IMAGE-BASED SEXUAL ABUSE CRIMINALISATION IN MEMBER STATES	14
3.1 Introduction	14
3.2 Identification of the relevant national criminal legislation: revenge porn, non-consensual pornography, and image-based sexual abuse	14
3.3 Key examples from selected national legal systems	15
3.4 Problematic aspects of including deepfake pornography in traditional revenge porn regulation.....	19
3.5 Final remarks	20
CHAPTER 4 - ENTERS THE EUROPEAN UNION: OUTLINES OF A COMMON FIGHT AGAINST DEEPPAKE PORNOGRAPHY	21
4.1 Introduction	21
4.2 The EU fight against gender-based violence: from the Gender Equality Standard to the Istanbul Convention.....	22
4.3 The Gender Violence Proposal and the Parliament's Legislative Resolution of 24 April 2024	24
4.4 Article 7(b): the Commission's plan to harmonize deepfake pornography criminalization	26
4.4.1 The content of Article 7 before and after the Parliament's Legislative Resolution: image-based sexual abuse and deepfake pornography	26
4.4.2 Problems of deepfake pornography harmonization.....	28
4.4.3 The legal basis problem.....	29
4.4.4 Threatening, inciting, aiding and abetting	30
4.4.5 Coordination with other European provisions	31
CHAPTER 5 – CONCLUSIONS	33

5.1 Answer to the research question.....	33
5.2 Limitations of the work and further research	33
BIBLIOGRAPHY.....	35
ANNEX: LIST OF NATIONAL LAWS AND THEIR TRANSLATION	41

CHAPTER 1 - INTRODUCTION

1.1 Background

Technology that allows the creation of new content or the manipulation of existing media is rapidly improving.¹ The next frontier of digital alteration is provided by Artificial Intelligence (AI). Of all the meanings that AI has, here the expression is used in relation to those machine-based systems that, given an explicit or implicit task and an input, infer conclusions by the analysis of the given data and choose the best course of action to achieve the goal.² Such a definition, albeit simplistic, has the advantage of restricting the focus on AI as a set of technologies, leaving aside unnecessary rhetorical readings.³

In the context of AI as an increasingly more accessible technology capable of producing highly realistic media, the term “deepfake” refers to “audio or visual media that seem authentic, and which feature people that appear to say or do something they have never said or done”.⁴ In other words, deepfake technology can be used to produce deceiving media, where the voices we hear and the faces we see are not authentic.⁵

This manipulation method owes its name to the fusion of “deep learning”, which is a type of machine learning technique employed in “training” AI, and “fake”, which refers to a characteristic of the media produced.⁶ Its functionalities have been deployed in the creation of movies and

¹ Danielle Keats Citron and Robert Chesney, ‘Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security’ (2019) 107 California Law Review 1753, 1757.

² The Organisation for Economic Co-operation and Development (OECD), acting in its capacity as an advisory body for public policies and international standard-setting (<<https://www.oecd.org/about/>>) has recently updated its Recommendation on Artificial Intelligence (OECD, *Artificial Intelligence in Society* (OECD Publishing, 2019)) to keep up with the rapid developments in the field. See OECD, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449 (2023) <<https://legalinstruments.oecd.org/en/instruments/oecd-legal-0449#mainText>>. See for a comment on the decision of the OECD to update its Recommendation: Luca Bertuzzi, ‘OECD updates definition of Artificial Intelligence “to inform EU’s AI Act”’ (*Euractiv*, 14 November 2023) <<https://www.euractiv.com/section/artificial-intelligence/news/oecd-updates-definition-of-artificial-intelligence-to-inform-eus-ai-act/>> accessed 27 April 2024. For another definition of Artificial Intelligence see also: High-Level Expert Group on Artificial Intelligence, ‘A Definition of AI: Main Capabilities and Disciplines’ (2019) <https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf> accessed 27 April 2024.

³ See Stan Franklin, *The Cambridge Handbook of Artificial Intelligence* (Cambridge University Press, Keith Frankish and William Ramsey 2014), Ch. 1 for an analysis of the evolution of the notion of AI.

⁴ European Parliamentary Research Service, ‘Tackling Deepfakes in European Policy’ (2021) PE 690.039 <[https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU\(2021\)690039_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf)> accessed 27 April 2024.

⁵ Under the AI Act as proposed by the Commission, “[u]sers of an AI system that generates or manipulates image, audio or video content that appreciably resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful (‘deep fake’), shall disclose that the content has been artificially generated or manipulated.” See Commission, ‘Proposal for a Regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts’ COM (2021) 206 final, Art. 52(3).

⁶ An overview of the technical aspects behind the deepfake can be seen in Amelia O’Halloran, ‘The Technical, Legal, and Ethical Landscape of Deepfake Pornography’ (BA Thesis, Brown Computer Science 2021), 12. A terminological clarification is in order: the term “deepfake” if used by itself could indicate the technology employed, the content produced, or even the social phenomenon. The ambivalence can result in textual obscurity. Clarification will be provided when such ambiguity could lead to doubts.

videogames, and to satire videos parodying politicians.⁷ Although many “prosocial” applications consecrate deepfake technology as a potentially beneficial one,⁸ the harms related to the misuse of this technology, both to society⁹ and to the individual,¹⁰ seem to surpass its benefits.¹¹

One domain where deepfake technology is massively developed and employed is the creation of pornographic content.¹² According to research published by Sensity AI in 2019, 96% of all deepfakes feature non-consensual pornography.¹³ The creation of deepfake pornographic content consists of the insertion of people’s faces and/or voices into real pornography.¹⁴

In times when deepfake was cutting-edge technology, only celebrities were the target.¹⁵ Though public figures remain the primary target (internet personalities, such as Twitch streamers, seem to be particularly exposed in recent news),¹⁶ widely available and accessible desktop tools can now be used by anyone to create sexual content featuring classmates, acquaintances, or even strangers.¹⁷ All that is needed are enough photos to “feed” the AI.¹⁸ In this respect, deepfake pornography is not a new phenomenon, but its expansion is unprecedented.¹⁹

The diffusion of websites dedicated to deepfake pornography and the spread of affordable apps have given a boost to the amount of material produced and to the number of those making use of it.²⁰

⁷ In 2018 Jordan Peel, a North-American comedian, superimposed his face to that of President Barack Obama, and with his likeness gave a “questionable” speech. The episode is reported by many, for instance, Benjamin Suslavich, ‘Nonconsensual Deepfakes: A “Deep Problem” for Victims’ (2022) Albany Law Journal of Science and Technology, forthcoming <<https://papers.ssrn.com/abstract=4137782>> accessed 27 April 2024, 3.

⁸ For instance, in the hands of educators, it could become an innovative and interesting pedagogical instrument, by recreating past events and giving life to historical figures. See Citron and Chesney (n 1) 1768-1769. Fake child pornography could be used to treat convicted paedophiles. See Bart van der Sloot, Yvette Wagenveld and Bert-Jaap Koops, ‘Deepfakes: The Legal Challenges of a Synthetic Society’ (2021) Tilburg Institute for Law, Technology, and Society <<https://www.tilburguniversity.edu/sites/default/files/download/Deepfake%20EN.pdf>> accessed 27 April 2024, 5. In the medical field, deepfake could help with voice creation for hard-of-hearing, deaf or mute people. See European Parliamentary Research Service (n 4) 28. For other examples of beneficial use of deepfake technology see Adrienne de Ruiter, ‘The Distinct Wrong of Deepfakes’ (2021) 34 Philosophy & Technology 1311, 1316.

⁹ A common concern is that deepfake might play a role in the spreading of fake news and misinformation: malicious manipulation of a video featuring a prominent politician could cause severe societal harm, by undermining trust, raising scandals, influencing elections, and starting wars.

¹⁰ Harm can affect the individual both in their finances and in their intimacy. See more in detail European Parliamentary Research Service (n 4) 29, table 2.

¹¹ This is the conclusion reached in Sloot, Wagenveld and Koops (n 8) 3.

¹² Indeed, the word “deepfake” itself was used for the first time in 2017 as the nickname of a Reddit user who altered pornographic videos using the faces of famous actresses. Edvinas Meskys and others, ‘Regulating Deep Fakes: Legal and Ethical Considerations’ (2020) 15 Journal of Intellectual Property Law & Practice 24.

¹³ Henry Ajder and others, ‘The State of Deepfakes: Landscape, Threats, and Impact’ (2019) <https://regmedia.co.uk/2019/10/08/deepfake_report.pdf> accessed 27 April 2024, 1.

¹⁴ Danielle Keats Citron, ‘Sexual Privacy’ (2019) 128 Yale Law Journal 1870.

¹⁵ Samantha Cole, ‘AI-Assisted Fake Porn Is Here and We’re All Fucked’ (*Vice*, 11 December 2017) <<https://www.vice.com/en/article/gdydm/gal-gadot-fake-ai-porn>> accessed 27 April 2024.

¹⁶ Samantha Cole, ‘“You Feel So Violated”: Streamer QTCinderella Is Speaking Out Against Deepfake Porn Harassment’ (*Vice*, 13 February 2023) <<https://www.vice.com/en/article/z34pq3/deepfake-qtcinderella-atric>> accessed 27 April 2024.

¹⁷ Miha Šepece and Melanija Lango, ‘Virtual Revenge Pornography as a New Online Threat to Sexual Integrity’ (2020) 15 Balkan Social Science Review 117, 120.

¹⁸ Citron and Chesney (n 1) 1772.

¹⁹ The problem is growing together with our use of social media: the more photos one shares, the easier it is for perpetrators to obtain the necessary material. Karolina Mania, ‘Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings From a Comparative Legal Study’ (2022) 0 Trauma, Violence, & Abuse 1.

²⁰ Moira Donegan, ‘Demand for deepfake pornography is exploding. We aren’t ready for this assault on consent’ (*The Guardian*, 13 March 2023) <<https://www.theguardian.com/commentisfree/2023/mar/13/deepfake-pornography-explosion>> accessed 27 April 2024.

Investigations into the numbers of deepfake pornography support the claim that the demand for this product is growing.²¹

1.2 Problem statement

Established that deepfake pornography is a growing problem, the role of criminal law is called into question. Indeed, some legal systems, such as certain states in the USA, have adopted forms of criminalization of deepfake pornography.²²

In the EU, the victim of a deepnude (that is, fake intimate material) would look at national criminal laws for protection, as the burden to identify criminally relevant conducts (traditionally) falls upon national legislators.²³ Member States usually punish the diffusion of non-consensual pornography, but they remain silent as far as deepfake pornography is concerned.²⁴ If criminal provisions concerning the former can encompass the latter, it is an object of debate.²⁵ If the outcome of this discussion was negative, laws on non-consensual pornography would not apply to deepfake pornography. Then, the problem would arise of figuring out how to protect the “deepfaked”, i.e. the person whose facial features are replicated into the pornographic material.

The perspective of the protection of the individual in its fundamental rights brings into play the role of the EU. It is true that EU institutions hold very limited competence in the area of substantive penal law,²⁶ and that they do not have the duty nor the aspiration to fill any gaps in the criminal substantive law of Member States (MSs).²⁷ Nevertheless, the role of the Union in criminal legislation, especially since the Treaty of Lisbon, has significantly evolved over time.²⁸ There is no doubt that the Union cannot create criminal norms immediately applicable throughout its territory. However, it is possible to refer to European criminal law as a process of convergence of national penal laws toward a common EU-promulgated rule.²⁹

Keeping this limitation in mind, it is worth wondering if and in what terms the Union can fulfil a function of guardianship of fundamental rights when national criminal laws struggle to do so.³⁰ More specifically, the EU-level criminalization of a behavior, such as deepfake pornography, that may go

²¹ Besides the already quoted report from the European Parliamentary Research Service (n 4), the same concern is expressed in an investigation launched by the Revenge Porn Helpline in the UK (the U.K. governmental service for adults experiencing intimate image abuse). The report, titled ‘Intimate image abuse, an evolving landscape’, is available at <https://revengepornhelpline.org.uk/assets/documents/intimate-image-abuse-an-evolving-landscape.pdf?_=1639471939>. As Mania (n 19) 2, points out, an 87% increase in cases of deepfake pornography has been registered in 2020. A BBC article reports that one website received 38 million visits in 2021. See Monika Plaha and Joseph Lee, ‘Sharing pornographic deepfakes to be illegal in England and Wales’ (BBC, 25 November 2022) <<https://www.bbc.com/news/technology-63669711>> accessed 27 April 2024. Another platform provides about 20,000 videos to 13 million monthly users. See Sarah McDermott and Jess Davies, ‘Deepfaked: ‘They put my face on a porn video’ (BBC, 21 October 2022) <<https://www.bbc.com/news/uk-62821117>> accessed 27 April 2024. Among women, the awareness of the possibility of unwillingly featuring a pornographic video is high. The findings of a survey published in 2021 by HateAid place at 30 the percentage of women who fear their stolen or faked pictures to be published on the Internet. See HateAid, ‘Boundless Hate on the Internet–Dramatic Situation across Europe’ (2021) <https://hateaid.org/wp-content/uploads/2022/04/HateAid-Report-2021_EN.pdf> accessed 27 April 2024.

²² Recently enacted provisions punish deepfake pornography in the States of Virginia, California and New York. For an overview of the criminalization of deepfake pornography in the United States, see O’Halloran (n 6).

²³ Peter Csonka and Oliver Landwehr, ‘10 Years after Lisbon – How “Lisbonised” is the Substantive Criminal Law in the EU?’ (2019) 4 *Eucrim* 261, 262.

²⁴ Mania (n 19) 4.

²⁵ As will be illustrated in the literature review, this debate has not yet ignited in European doctrine. For the debate in the USA see Douglas Harris, ‘Deepfakes: False Pornography Is Here and the Law Cannot Protect You’ (2019) 17 *Duke Law & Technology Review* 99, 123.

²⁶ Csonka and Landwehr (n 23) 262.

²⁷ Merita Kettunen, *Legitimizing European Criminal Law* (Springer 2020) 51.

²⁸ Valsamis Mitsilegas, *EU Criminal Law* (Hart Publishing 2022) 30.

²⁹ Kettunen (n 27) 67.

³⁰ Mitsilegas (n 28) 45.

unpunished under national criminal law, has to be examined in light of the recent Proposal for a Directive on violence against women and domestic violence (hereinafter: Gender Violence Proposal), which aims to do so.³¹

1.3 Research question and sub-questions

The aim of this research can be expressed in the following research question: "Can the European Union's response to deepfake pornography make up for the absence of criminal liability in Member States?" The answer will be reached through the following sub-questions:

1. What is deepfake pornography, and what are the difficulties of identifying a clear definition?
2. Are current national laws criminalizing image-based sexual abuse suitable to be extended to deepfake pornography, or should criminal liability for the latter be considered absent in national jurisdictions lacking a specific provision for deepfake pornography?
3. To what extent would the proposed Directive on violence against women and domestic violence make up for the general absence of criminal liability for deepfake pornography in Member States?

1.4 Literature review

Since deepfake is a technology that presents as many applications as problems, academic literature on the topic is abundant. Scholars have debated both the positives and the potential issues that deepfake content could cause to society, trying to provide an overview of its impact on information and security, and the connected legal and ethical challenges.³² Public institutions show an increasing level of awareness; for instance, in July 2021 the European Parliamentary Research Service published a report that assessed the technical, societal, and regulatory aspects of deepfake technology.³³

Nevertheless, deepfake pornography has not piqued the interest of legal scholars. On the contrary, there is a concerning lack of European scholarship, and little research has been carried out on the European response to deepfake pornography as a criminal phenomenon.³⁴ This is the gap that this research intends to fill.

First of all, there is an overall lack of research on what exactly is the concerned behavior: does it entail exclusively the creation of deepfake content, or does it extend to its dissemination? Who are those involved in such activities? Who are the victims? In the USA, a conspicuous doctrinal thread addressed these issues starting from the work of Danielle Keats Citron on the notion of "Sexual Privacy".³⁵ Their analysis of the legal and technical complexities of deepfake pornography is valuable for our purposes.

Research on this topic is strictly connected to non-consensual pornography and revenge pornography, which further complicates definitory efforts.³⁶ These phenomena are indeed intimately related, but the nature of their relationship is debated. In literature, non-consensual pornography and

³¹ Commission, 'Proposal for a Directive of the European Parliament and of the Council 2022/0066 of 8 March 2022 on combating violence against women and domestic violence' COM/2022/105 final.

³² An overview is given in van der Sloot, Wagensveld and Koops (n 8).

³³ European Parliamentary Research Service (n 4).

³⁴ Only Carlotta Rigotti and Clare McGlynn, 'Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission's proposal to criminalise image-based sexual abuse' (2022) 13 *New Journal of European Criminal Law* 452.

³⁵ Citron (n 14). Another widely quoted research from the same author is Citron and Chesney (n 1). A similar academic attention can be found in Canada. For a review of the Canadian policy on deepfake pornography see Vasileia Karasavva and Aalia Noorbhai, 'The Real Threat of Deepfake Pornography: A Review of Canadian Policy' (2021) 24 *Cyberpsychology, Behavior, and Social Networking* 203.

³⁶ For instance, Mania (n 19) addresses the problem of deepfake pornography under the lens of revenge porn.

revenge porn are frequently seen as synonyms and used interchangeably.³⁷ Other times, the former is interpreted as the *genus*, a broad category where the only element required is the lack of consent, but that does not say much about actors and conduct.³⁸ Accordingly, revenge porn is defined as a *species* of the *genus* non-consensual pornography, consisting of divulging the received intimate material without consent or legitimate purpose.³⁹ Therefore, it does not concern the activity of forging, unlike deepfake pornography, which therefore is a different *species* of the same *genus* of non-consensual pornography.⁴⁰

As an alternative reconstruction, it has been proposed to absorb the notion of non-consensual pornography in the better-known category of revenge porn, and to distinguish between “old fashion revenge porn” (i.e. the “classic” conduct of non-consensual pornography) and “virtual revenge porn”.⁴¹ This reading is not common in literature. Besides, the expression “revenge porn” includes an element of retaliation that is not necessarily present in situations of deepfake pornography, so it appears less suitable to comprehend it.⁴²

Again, it is necessary to resort to US literature. Regulation of deepfake pornography exists only in a minority of North American States, and federal law is absent.⁴³ Where norms lack, US authors have speculated on the possibility to perform a flexible interpretation of (what they refer to as) “revenge porn laws” to include the creation of deepfake pornographic media, but they have concluded against this extension.⁴⁴ The main reason is that revenge porn statutes punish the distribution of intimate material without the consent of the person depicted, whereas with deepfakes the actual intimacy of the victim is not divulged.⁴⁵

As it is by now evident, this research will have to rely heavily on the work of North American scholars. Nevertheless, significant structural differences prevent a plain comparison between the European and North American legal approaches to deepfake pornography. First, the legal categories used to evaluate the problem differ considerably. For instance, the discussion in the USA often revolves around the extent of the protection offered by the First Amendment to perpetrators of deepfake pornography.⁴⁶ Second, the peculiar nature of the EU as a legislator differentiates it from the federal North American system and requires different considerations on the sources of the law.⁴⁷ Ultimately, these limitations make a comparison less profitable but do not invalidate it.

Research has focused on the possibility and the modality of regulating deepfake pornography. A few authors proposed legal responses different from criminal law (defamation, privacy, or copyright infringement laws),⁴⁸ or non-legal responses, such as filtering user-generated content on social media

³⁷ Danielle Keats Citron and Mary Anne Franks, ‘Criminalizing Revenge Porn’ (2014) 49 Wake Forest Law Review 345, 346.

³⁸ Rebecca Delfino, ‘Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn’s Next Tragic Act’ (2019) 88 Fordham Law Review 887, 896.

³⁹ Mary Anne Franks, ‘Drafting an Effective “Revenge Porn” Law: A Guide for Legislators’ (2015) <<https://ssrn.com/abstract=2468823>> accessed 27 April 2024.

⁴⁰ As clarified by Delfino (n 38) 896.

⁴¹ Šepece and Lango (n 17).

⁴² Franks (n 39) 2.

⁴³ O’Halloran (n 6).

⁴⁴ See Harris (n 25) 103; Anne Pechenik Gieseke, “‘The New Weapon of Choice’: Law’s Current Inability to Properly Address Deepfake Pornography’ (2020) 73 Vanderbilt Law Review 1479, 1501ff; for the Canadian system, see Jane Bailey and others, ‘AI and Technology-Facilitated Violence and Abuse’, *Artificial Intelligence and the Law in Canada* Florian Martin-Bariteau & Teresa Scassa eds (Toronto: LexisNexis Canada 2021).

⁴⁵ See Gieseke (n 44).

⁴⁶ Citron (n 14) 1936; Gieseke (n 44) 1489; Harris (n 25) 104; Suslavich (n 7) 18.

⁴⁷ Mania (n 19) 3.

⁴⁸ See for instance Suslavich (n 7).

platforms.⁴⁹ Since our purpose is limited to penal considerations, this literature will only partially be considered.

The attention of European scholarship generally falls upon current national criminal provisions, with the aim of understanding if they fall short in addressing deepfake pornography. However, in doing so, an exclusively national perspective is adopted, with the risk of narrowing down the problem excessively.⁵⁰ Few studies perform a comparative analysis of European national legal systems.⁵¹

No research has been published on a unitary European approach to deepfake pornography as a criminal phenomenon. The idea of European criminal legislation has always been perceived as problematic yet fascinating and, to a certain extent, even necessary.⁵² Over the years, the debate has undergone drastic changes in perspective, together with societal and political developments.⁵³ The Treaty of Lisbon has redefined the role of the Institutions and opened a new chapter in the dialogue on EU criminalisation. Since then, the issue has taken the shape of a cautious academic debate⁵⁴ on the possibility of theorizing an actual competence of the Union in criminal substantive matters, and on the limits of said competence.⁵⁵

Nowadays, contributions are published with the explicit goal of legitimising EU criminalisation.⁵⁶ The topic is discussed from the perspective of the legal basis allowing EU Institutions to promulgate substantive criminal regulations (Article 83 TFEU)⁵⁷ but also the type of regulatory instrument through which that can happen (directives).⁵⁸

Amidst the doctrinal debate, EU Institutions have played their new role by promulgating directives. They touched upon the problem of deepfake pornography in criminally relevant directives related to two different fields. First, the protection of the child, where the notion of “pornography” adopted by the EU is broad. For instance, Article 2(iv) of the Directive 2011/92/EU⁵⁹ define “child pornography” as (any) “realistic images of a child engaged in sexually explicit conduct [...]”, potentially extending to deepfake-generated content. Second, gender-based violence: in the Commission proposal for a Directive on this topic, the fabrication of deepfakes is explicitly included in Article 7(b).⁶⁰

⁴⁹ Tyrone Kirchengast, ‘Deepfakes and Image Manipulation: Criminalisation and Control’ (2020) 29 Information & Communications Technology Law 308, 320.

⁵⁰ Two Master’s theses from Tilburg Law School have addressed this issue in recent times. One focuses on how the Dutch legal system could fight deepfake pornography (Daphne Stevens, ‘Regulating Deepfake Technology - Legislative possibilities in the Netherlands to obstruct the use of deepfake technology for the creation of non-consensual pornography’ (Master thesis, Tilburg Law School 2020)). The other analyses the Italian context with the same purpose (Andrea Rizzica, ‘Sexually explicit deepfakes: to what extent do legal responses protect the depicted persons? - Analysis of the Italian scenario through criminal law, data protection law and right to image’ (Master thesis, Tilburg Law School 2021)).

⁵¹ Mania (n 19); Sepece and Lango (n 17); Rigotti and McGlynn (n 34). See also the Commission’s report: Sara De Vido and Lorena Sosa, *Criminalisation of gender-based violence against women in European States, including ICT-facilitated violence* (Publications Office of the European Union 2021).

⁵² Geert Corstens and Jean Pradel, *European Criminal Law* (Kluwer Law International 2002) 6.

⁵³ The matter is discussed in a diachronic perspective in a recent contribution that examines the evolution from a merely economic union, all the way to the Treaty of Lisbon. See Mitsilegas (n 28).

⁵⁴ Doctrinal, yet heavily influenced by political considerations. Kettunen (n 27), VI

⁵⁵ Helmut Satzger, *International and European criminal law* (Hart/Nomos 2018); André Klip, *European criminal law: an integrative approach* (Intersentia 2021); Helmut Satzger, ‘The Harmonisation of Criminal Sanctions in the European Union - A New Approach’ (2019) 2 Eucrim 115; Csonka and Landwehr (n 23).

⁵⁶ For instance Kettunen (n 27).

⁵⁷ Consolidated version of the Treaty on the Functioning of the European Union, 2008/C 115/01, Article 83(1).

⁵⁸ Anabela Miranda Rodrigues, ‘Fundamental Rights and Punishment: Is There an EU Perspective’ (2019) 10 New J Eur Crim L 17.

⁵⁹ Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA.

⁶⁰ Gender Violence Proposal, Article 7(b).

1.5 Methodology and overview of the chapters

This research aims to assess the current state of criminal law responses to deepfake pornography in European Member States, and subsequently to discuss how the European Union has regulated and plans to harmonize this field.

All considerations related to the nature and the notion of deepfake pornography are condensed in Chapter 2, where an answer to sub-question 1 will be provided through the analysis of relevant doctrinal contributions. This section will debate the notion of deepfake pornography as the product of a specific technique, as a socially relevant phenomenon, and as a morally objectionable behaviour. Sources have been selected accordingly. For section 2.2, contributions regarding the technical functioning of deepfakes are used. The chosen studies are a number of legal and/or sociological contributions, mainly by U.S. authors, selected because they are recent and because they are particularly focused on describing the technological aspects of deepfake pornography. In section 2.3, the description of deepfake pornography as a sociological phenomenon is based on those few empirical criminological studies, including victimization and perpetration surveys, that concern it. As for section 2.4, among all the studies on deepfakes in general, only those were selected that had some relevance to the moral implications of deepfake pornography, and in particular that provide a clear picture about the issue of possession, creation, and distribution of virtual pornography, and why one or more of these behaviours is ethically objectionable.

Chapter 3 will deal with sub-question 2. Doctrinal fundamental studies have been examined in section 3.2 to establish the object of the comparative research, which is carried out in section 3.3 as an assessment of the current state of criminal law responses to image-based sexual abuse in Europe. To do so, examples of national legislation criminalizing revenge pornography will be given. The choice was made not to conduct an all-encompassing survey involving all Member States. First, because it would have taken too much time and resulted in the production of an excessively long section. Second, because it would have been unprofitable to this research, which is not intended to probe and catalogue all national criminal legislation related to deepfake pornography, but rather to provide examples of how the latter may be treated in Member States' legal systems. The fourteen states whose criminal laws were examined were chosen because of the simultaneous presence of two elements: the existence of well-defined criminal liability for at least one form of image-based sexual abuse, and the availability not only of the legislation itself, but also of sufficient doctrinal reflection to support the analysis conducted here. Finally, in section 3.4 the problematic aspects of trying to include deepfake pornography under image-based sexual abuse national regulations are illustrated. Such analysis will rely on the doctrinal sources identified in Chapter 2, but will also require the conceptual effort of comparing two legal notions.

Having defined the current state of the criminal law fight against deepfake pornography in MSs, Chapter 4 will provide an answer to sub-question 3. In section 4.2, the discussion will fall on the current legal framework of the EU regulatory responses to deepfake pornography. To this end, textual analysis of the relevant programmatic and political documents will be conducted, together with the study of the few available doctrinal contributions. The content of the Gender Violence Proposal will be illustrated in section 4.3 through black letter analysis of the text. Finally, in section 4.4, the discussion will move on to the limits and problems of the provision targeting deepfake pornography in the Gender Violence Proposal, with particular attention to the legal basis for the intervention (Article 83(1) TFEU). Scarce legal research on this part will be accompanied by black letter analysis of the Proposal and the studies conducted by the European Parliament and the European Economic and Social Committee.

In Chapter 5, conclusions are given. After the tentative answer to the research question, final considerations on the limitations of the work and on future lines of research are provided.

CHAPTER 2 - NOTION AND FEATURES OF DEEPPAKE PORNOGRAPHY

2.1 Introduction

To further clarify what is under analysis in this research, it is essential to draft a working notion. This chapter, therefore, outlines the problems that arise when a common notion of “deepfake pornography” is sought. Three critical aspects will singularly be addressed in a different section (2.2, 2.3 and 2.4). In the final part, they will be brought together for conclusive remarks on the concept of deepfake pornography (section 2.5).

2.2 Deepfake pornography as the misuse of a technology

The first aspect to be underlined is that, while the term “pornography” refers to the nature of the content, “deepfake” refers to the technology.⁶¹ So, to identify a precise notion of deepfake pornography is, in the first place, to explain what deepfake technology is. To this end, technical features are now presented.

Because the human face contains such a level of detail, to give a machine all the information necessary to reproduce it (for instance, the exact distance between the eyes or their color) would be virtually impossible.⁶² That is why “machine learning” comes into play.⁶³ Technically speaking, machine learning is not a technology in itself, but an umbrella term that identifies a certain “approach”.⁶⁴ This approach, by which the machine “learns” something, is particularly useful for tasks, such as determining what an image represents, where a pattern can be detected from a series of examples.⁶⁵ By “feeding” pictures representing the likeness of a person (input) to systems of this type, they can detect and reproduce the corresponding facial features (output). This is why the more diverse input provided, the more accurate the output will be.⁶⁶

The machine learning systems that have been applied to generate deepfake videos are neural networks,⁶⁷ which owe their name to the similarities between the way processing units interact in these systems and the way synapses form connections in the brain.⁶⁸ Nowadays, the use of Generative Adversarial Networks (GANs) has allowed the creation of easier-to-make and more realistic videos by using simultaneously two neural networks. One creates the fake output (“generator”), and the other evaluates if the output is believable (“discriminator”). These two neural networks, by “competing”, greatly improve the quality of the outcome.⁶⁹

⁶¹ Pornography can be intended here in its broad meaning, that of any “sexually explicit material primarily intended to produce sexual arousal”. Literally in Daniel Story and Ryan Jenkins, ‘Deepfake Pornography and the Ethics of Non-Veridical Representations’ (2023) 36 *Philosophy & Technology*, 2.

⁶² O’Halloran (n 6) 12.

⁶³ Suslavich (n 7) 163.

⁶⁴ Franklin (n 3) 26; HLEG (n 2) 3.

⁶⁵ HLEG (n 2) 3.

⁶⁶ Johnny Botha and Heloise Pieterse, ‘Fake News and Deepfakes: A Dangerous Threat for 21st Century Information Security’ (15th International Conference on Cyber Warfare and Security, Old Dominion University, Norfolk, USA, March 2020). However, it should be remembered that hundreds of frames can be obtained from a single video.

⁶⁷ See O’Halloran (n 6) 13, for the description of the early way deepfakes were produced, so-called “Encoder-Decoder Pairs”.

⁶⁸ HLEG (n 2) 4. Then, the ability of a system to solve tasks depends. For instance, the more “nodes”, or “layers” are included in this process, the more complex tasks can be assigned to the system. See Suslavich (n 7) 169.

⁶⁹ Meskys and others (n 12) 3.

Although this may sound complicated and even mysterious, in practice coding a deepfake model requires more patience (the whole process may take up to a few days)⁷⁰ than technical skills or expensive equipment.⁷¹

What has been described in this subsection is the only face-swapping technique employed in the creation of realistic pornography.⁷² In conclusion, deepfake pornography is uniquely linked to and defined by a technique. In this sense, it seems to be connected exclusively to the misuse of a specific technology.

2.3 Deepfake pornography as a social phenomenon

In general, research on features and numbers of criminal phenomena with a (prevalent or exclusive) digital dimension, such as deepfake pornography, suffers from an increased difficulty of collecting information on victims, perpetrators, and behaviors.⁷³ In particular, deepfake pornography is a complex social phenomenon, one that criminological research has yet to dissect.⁷⁴ Notwithstanding these limitations, an investigation of deepfake pornography's actors and victims is here necessary.

Deepfake pornography is thought for a typically male audience, which has the choice to watch content that someone else has distributed on a platform or create the deepfake themselves. For this purpose, they can use programs like FaceApp that simply require a video of the person to be deepfaked,⁷⁵ or even train a deepfake model, which, as illustrated in the previous sub-section, does not require particular skills or technical means. Next to the "occasional" user of AI pornography, there are also those who habitually create and/or distribute it.⁷⁶

While men are typically the audience and creators, women are the almost exclusive target.⁷⁷ Under-reporting, due to victims being unaware or unwilling to report, renders estimates on the number of victims inaccurate.⁷⁸ It is important to notice that in every deepfake, two persons are victimized: not only the deepfaked, i.e. the person whose face (and voice) have been superimposed, but also the actor in the original video, who most likely did not agree to such modification of her features.⁷⁹

Sexual gratification is of course the immediate reason why deepfake pornography is watched.⁸⁰ However, it is only the most evident of the elements to be considered: behind the creation or the dissemination of fake pornography, not unlike the distribution of "real" intimate material, the reasons and the contexts vary.⁸¹

⁷⁰ O'Halloran (n 6) 16.

⁷¹ Besides, the tools necessary to create these models are freely available to developers. Gieseke (n 44) 1487.

⁷² Botha and Pieterse (n 66).

⁷³ Bert-Jaap Koops, 'The Internet and its Opportunities for Cybercrime' (2010) Tilburg Law School Legal Studies Research Paper Series No. 09/2011, 738.

⁷⁴ A criminological investigation is carried out in Asher Flynn and others, 'Deepfakes and Digitally Altered Imagery Abuse: A Cross-Country Exploration of an Emerging form of Image-Based Sexual Abuse' (2022) 62 The British Journal of Criminology 1341. More in general on the social phenomenon of technology-facilitated sexual abuse: Nicola Henry and Anastasia Powell, 'Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research' (2018) 19 Trauma, Violence, & Abuse 195.

⁷⁵ Carl Öhman, 'Introducing the pervert's dilemma: a contribution to the critique of Deepfake Pornography' (2020) 22 Ethics and Information Technology 133.

⁷⁶ For example, the occurrence of poly-creation is higher than single-creation in Flynn's survey. See Flynn (n 74) 1348.

⁷⁷ Citron and Chesney (n 1) 1773. Story and Jenkins (n 61) 3, report that a small number of deepfakes feature males, although only celebrities, and not, as it happens for females, also non-famous people. The results of Flynn's survey seem to contradict the statement that women are more likely to be victims, suggesting instead a higher victimization rate in men. However, as explained by the author, the results should be doubted, as they are not reflected in their qualitative investigative nor any other analysis of online deepfake content. See Flynn (n 74) 1350.

⁷⁸ Rigotti and McGlynn (n 34) 458

⁷⁹ Delfino (n 38) 898.

⁸⁰ Citron and Chesney (n 1) 1772.

⁸¹ Flynn (n 74) 1341.

First, not all the deepfake pornography generated is also distributed.⁸² And when it is, studies show that reaching an audience as broad as possible is often not the goal of the creator or the person sharing it.⁸³ When dissemination does occur (or is threatened) it could be done to harm the deepfaked or someone close to him/her, for instance by causing psychological distress.⁸⁴ But it can also be part of a wider attack.⁸⁵ A deepfake can be used for material gain, as a form of “sextortion”: the victim is shown the altered video, and is forced to choose between its publication and giving in to the demands, such as sharing intimate material or paying money.⁸⁶ It could also be part of a strategy to undermine trust in a public figure. A politician could be defamed by appearing engaged in sexual activities,⁸⁷ and a journalist can be deprived of her credibility.⁸⁸

To conclude, deepfakes can be made for many reasons, and harming the victim is only one of them. From a sociological perspective, deepfake pornography is a heavily gendered phenomenon,⁸⁹ which fits into a scheme of gender oppression and inequity.⁹⁰ However, the discussion on the extent and features of deepfake pornography as a criminological phenomenon suffers from the scarcity of victimization and perpetration investigations.⁹¹

2.4 The distribution, creation, and possession of deepfake pornography as morally objectionable behaviors

From what has been discussed so far, it is clear that the phenomenon of deepfake pornography has a strong negative connotation. Although from an ethical perspective it is not immediately identifiable where its wrongfulness lies, it is its wrongfulness (or more accurately, the wrongfulness of certain conducts related to deepfake pornography) that must be discussed. In this sense, at this stage, what is pursued here is to understand what aspect/s of deepfake pornography is/are harmful.⁹²

Let us take as an example virtual child image-based sexual abuse (or, to use the language of the Cybercrime Convention, virtual child pornography).⁹³ In itself, it is a phenomenon that our society does not approve of, and because of this, states use criminal law to identify certain harmful conducts and punish perpetrators.⁹⁴ This is why, for instance, the act of producing child pornography for the purpose of its distribution is criminalized under the Cybercrime Convention.⁹⁵ Yet there are conducts

⁸² *ibid* 1346, reads that among the respondents to the investigation conducted, 11.3% reported the creation, 10.4% the distribution, and 10.1% the threat to distribute, and that poly-victimization (i.e. the simultaneous occurrence of two or three between these situations) was at 7.7%.

⁸³ Milena Popova, ‘Reading out of context: pornographic deepfakes, celebrity and intimacy’ (2020) 7 *Porn Studies* 367.

⁸⁴ Citron and Chesney (n 1) 1774.

⁸⁵ Citron (n 14) 1921.

⁸⁶ A news report led the Italian Data Protection Authority to warn about the emergence of this phenomenon. See Guido Scorza, ‘L’Fbi lancia l’allarme: porno-criminali in azione’ (*HuffPost*, 12 June 2023)

<https://www.huffingtonpost.it/rubriche/governare-il-futuro/2023/06/12/news/lfb_lancia_lallarme_porno-criminali_in_azione-12361450/> accessed 27 April 2024.

⁸⁷ See on the Italian Prime Minister Giorgia Meloni: Antonio Di Noto, ‘Mettono online video porno fake col volto di Meloni, a processo padre e figlio. La premier chiede 100mila euro: «Andranno in beneficenza»’ (*Open*, 24 October 2023) <<https://www.open.online/2023/10/24/sassari-deepfake-meloni-processo-richiesta-risarcimento/>> accessed 27 April 2024.

⁸⁸ See Citron (n 14) 1922-1923, on the case of Indian journalist Rana Ayyub.

⁸⁹ Öhman (n 75) 133-134.

⁹⁰ Citron (n 14) 1924.

⁹¹ Empirical studies on technology-facilitated sexual violence have been conducted mainly from the perspective of child abuse, so not much information is available on adult victimization and perpetration. Henry and Powell (n 74) 196.

⁹² Kettunen (n 27) 47.

⁹³ Council of Europe, Convention on Cybercrime, 23 November 2001, art 9.

⁹⁴ Yaman Akdeniz, *Internet Child Pornography and the Law: National and International Responses* (Milton: Taylor & Francis Group 2008) 4.

⁹⁵ Cybercrime Convention, art 9(1)(a).

within the context of virtual child pornography whose criminalization is controversial, such as the possession of the same material.⁹⁶

As for deepfake pornography, the problem of “how” exactly it is harmful is starting to get attention.⁹⁷ Not unlike the legal regime of virtual child pornography under the Cybercrime Convention,⁹⁸ let us start from the premise that all the conducts related to the creation, dissemination, and possession of deepfake pornography are harmful, and assess the correctness of this statement from an ethical perspective.

First, it could be argued that, because it implies sharing falsified information about someone, the distribution of fake pornographic material is in itself defamatory. And deepfake technology is indeed meant to produce fake material.⁹⁹ However, the problem of deepfake pornography is not one of authenticity. Unlike other contexts (think about the deepfake of a politician inciting riots), here the fake content is not spread to deceive the viewers. Many platforms even warn potential viewers that the content *is* fake.¹⁰⁰ Therefore, in the context of pornography, disseminating fake content is not necessarily defamatory.¹⁰¹

Instead, the problem lies in the fact that to distribute a deepfake is a form of “digital persona plagiarism”: to have someone’s face and/or voice “stolen” and introduced in a pornographic video means changing the way they are perceived in society.¹⁰² In other words, deepfake pornographic videos “hijack people’s sexual and intimate identities”, forcibly presenting them in a different way than the one intended by the deepfaked.¹⁰³ Therefore, nonconsensual dissemination is wrong.¹⁰⁴

Can the same be said about the creation of deepfake pornography, regardless of its distribution?¹⁰⁵ The problem here lies within the fact that, unlike child abuse, deepfakes are by nature “not real”.¹⁰⁶ They can be described as virtual pictures created using available information as input, and so as a sort of fantasy. And yet, fantasies of a sexual nature are normally considered admissible.¹⁰⁷ This is the so-called “pervert’s dilemma”.¹⁰⁸

One could argue that the difference lies in the fact that these fantasies are actually “created”, and that creation in itself manifests a more “evil” tendency. However, two arguments challenge this conclusion. The first is that, as illustrated in section 2.2, little more than uploading a single video in

⁹⁶ See on this debate Marie Eneman, Alisdair A. Gillespie and Bernd Carsten Stahl, ‘Criminalising fantasies: the regulation of virtual child pornography’ (2009) <https://www.researchgate.net/publication/265357703_CRIMINALISING_FANTASIES_THE_REGULATION_OF_VIRTUAL_CHILD_PORNOGRAPHY> accessed 27 April 2024.

⁹⁷ See for instance: Carl Öhman (n 75); Story and Jenkins (n 61); de Ruiter (n 8).

⁹⁸ Cybercrime Convention, art 9.

⁹⁹ And for this it is morally “suspect”. However, as illustrated in Chapter 1.1, deepfake technology can be employed for applications defined as “pro-social”. This makes it not intrinsically wrong. See de Ruiter (n 8) 1313. The author’s position on deepfake (in general, not with exclusive regard to pornography) is further articulated on page 1318ff.

¹⁰⁰ Story and Jenkins (n 61) 3. Popova’s findings (n 83) on deepfake pornography communities support this consideration.

¹⁰¹ However, the stigma still associated with pornography can still affect the opinion that society has of the deepfaked. See Story and Jenkins (n 61) 7-8.

¹⁰² de Ruiter (n 8) 1324.

¹⁰³ Citron (n 14) 1921.

¹⁰⁴ See Story and Jenkins (n 61) 9 for the formulation of the “Non-Veridical Representation Principle (NVRP)”. An exception could be made for “artistic” deepfake pornography. As speculated by Harris (n 25) 127, in theory, a person could consent to be represented in a sexual/intimate way through deepfake technology, even if that is usually not the case. In these situations, the representation would be non-veridical, but still not morally objectionable.

¹⁰⁵ More research has been carried out on diffusion than creation of deepfake pornography. Flynn (n 74) 1343.

¹⁰⁶ Or at least, unlike “traditional” virtual child abuse. Keep in mind that under art 9(2)(c) Cybercrime Convention the term “child pornography shall include pornographic material that visually depicts [...] realistic images representing a minor engaged in sexually explicit conduct”, thus including AI-generated content.

¹⁰⁷ With due exceptions. Story and Jenkins (n 61) 5, argue that in certain situations, such as a boss-employee relationship, fantasies of a sexual nature are wrong.

¹⁰⁸ This moral dilemma is introduced by Öhman (n 75) 134.

an App or a website is required to create a deepfake. Therefore, even if significant labour was, in fact, the manifestation of ill intent, this would not apply to the creation of deepfake pornography, because such labour is not always there. The second, which rests on a moral ground, is that it is not clear how materiality can justify this difference. At best, a “materialised fantasy” is ethically more problematic than a non-materialised one because materiality is a necessary premise for sharing: simple fantasies cannot be shared because they do not exist in a material form. However, this would not solve the pervert’s dilemma, because the problem of moral admissibility of deepfakes remains even in the absence of sharing.¹⁰⁹

A possible solution to the pervert’s dilemma is the following. On an abstract level, there is no difference between fantasies and deepfake porn. It is the context that plays a decisive role. Unlike the former, the latter, as illustrated in the previous sub-section, is a highly gendered phenomenon. In this sense, deepfakes become a form of virtual violence and perpetrate a scheme of gender inequity.¹¹⁰ So in conclusion, while creating a single fake video would be ethically permissible, it constitutes a problem in the context of gender violence.¹¹¹

Finally, is individual possession of deepfake porn wrong? Doctrinal reflection on the matter is scarcer, so it is harder to answer.¹¹² Possession for individual use, it could be argued, might lead to other, more “real” behaviours.¹¹³ Yet the same can be said about sexual fantasies, which, as argued above, are not to be condemned in themselves.¹¹⁴ In the end, unlike the behaviour of creating or distributing deepfake pornography, possessing it does not seem morally questionable.

2.5 Final remarks

This Chapter has so far illustrated how the notion of deepfake pornography is hard to delimit. First, considering what deepfake approach consents, deepfake pornography is limited to one form of face-swapping technique (section 2.2). Second, from a sociological perspective, deepfake pornography is clearly a part of the macro-phenomenon of gender violence, but extensive victimization and perpetration investigations are yet to be conducted (section 2.3). Third, an ethical approach suggests that both the creation and dissemination of deepfake pornography are morally wrong, but the discussion leaves out other important considerations, such as the wrongfulness of possession (section 2.4). This final subsection pulls together the strings and draw some conclusions on the problematic nature of the notion of deepfake pornography.

Neural networks are the only technology that allows for the rapid, easy, and widely accessible creation of fake high-quality output.¹¹⁵ These features set deepfake technology on another level from any other technology. Nevertheless, digital alteration and creation of fake pornography content can happen by means of different, more “rudimental” tools, such as Photoshop.¹¹⁶ So, is the alteration of a pornographic video via AI face-swapping techniques ontologically different from any other form

¹⁰⁹ *ibid.*

¹¹⁰ *ibid.*

¹¹¹ *ibid* 138. *Contra*: Harris (n 25) 127, argues that producing deepfake should not be made illegal for the same reason hammers are not prohibited, even if they can be used to commit manslaughter: it is sufficient to prohibit murder (deepfake dissemination, in the analogy).

¹¹² de Ruiter (n 8), Story and Jenkins (n 61), and Öhman (n 75) do not address it. A possible explanation is that it is a problem of legal rather than moral significance. This would explain why Harris (n 25) 127-128 addresses it. The author argues that illegal harms are confined to deepfakes that are disseminated, and that, according to the Supreme Court’s interpretation of the Constitution, “the sacrosanctity of what happens in the privacy of one’s home will likely protect the creation of deepfakes”.

¹¹³ This argument is commonly understood as the moral basis underlying the punishment of virtual child pornography possession. See Eneman, Gillespie and Stahl (n 96).

¹¹⁴ Story and Jenkins (n 61) 5.

¹¹⁵ Botha and Pieterse (n 66).

¹¹⁶ Clare McGlynn and Erika Rackley, ‘Image-Based Sexual Abuse’ (2017) 37 Oxford Journal of Legal Studies 534, 540. It is hard to imagine the use of similar tools to modify entire videos, but it is entirely possible for pictures.

of digital creation or alteration of a pornographic nature? Another way to ask this question is: is all fake pornography wrong, or only if sophisticated tools allow the production of highly realistic content?

As illustrated in section 2.4, it is not because of its ability to deceive that deepfake pornography is morally wrong. Therefore, the quality of the content and the degree of realism cannot be the parameters for moral questionability of face-swapping techniques.¹¹⁷

To add to that, anyone with a tool for digital drawing can create a sexual representation of someone. Although this does not imply alteration but creation, it does not seem less problematic than modifying an existing picture or video. In all these cases, the outcome is the same: there is a victim who sees him/herself represented in a sexualised manner against their will.

Then, the expression “deepfake pornography” is misleading because too narrow, and it risks demonizing the misuse of a specific technology losing track of the broader problem of fake image-based digital abuse. Then, either a more general expression, such as “image-based sexual abuse by means of digitally altered content”, is adopted,¹¹⁸ or, as it will be done in this research, the label “deepfake pornography” must be applied to every form of digitally created or altered image abuse,¹¹⁹ knowing that deepfake technology is the most advanced but not the sole one.¹²⁰

To conclude, a way to describe deepfake pornography for the purposes of this research is the following: deepfake pornography is a criminologically relevant phenomenon where image abuse happens through the production and distribution of fake pornography created primarily, but not exclusively, thanks to machine learning techniques.

¹¹⁷ Creating an obscene drawing of a woman with pen and paper is different from using advanced technology, *in primis* deepfake, because it does not fit in the context of gender violence. Öhman (n 75) 138.

¹¹⁸ The expression “image-based sexual abuse” has been proposed by McGlynn and Rackley (n 116) as an alternative to non-consensual pornography and revenge porn, and will be explored in section 3.2.

¹¹⁹ See also Flynn (n 74) 1342, for similar considerations.

¹²⁰ Citron and Chesney (n 1) 1757.

CHAPTER 3 - A COMPARATIVE PERSPECTIVE ON CURRENT IMAGE-BASED SEXUAL ABUSE CRIMINALISATION IN MEMBER STATES

3.1 Introduction

The goal of this Chapter is to provide an answer to subquestion 2 by determining the current state of criminalization of deepfake pornography in national legislation of European Member States (MSs). After a first part dedicated to selecting relevant national criminal legislation (section 3.2), the search will focus on image-based sexual abuse criminalisation in selected national systems (section 3.3). The results of this investigation will provide the foundations to discuss the shortcomings of these provisions when applied to deepfake pornography (section 3.4). The Chapter will be closed by some concluding remarks on the identified tendencies and recurring issues (section 3.5).

3.2 Identification of the relevant national criminal legislation: revenge porn, non-consensual pornography, and image-based sexual abuse

As a starting point, it must be noticed that MSs tend to not regulate deepfake pornography and that EU institutions have not played a harmonising role (yet).¹²¹ It could be, however, that broader or related provisions are in place in national jurisdictions. Therefore, the question to be asked is: is there a category of criminal offences encompassing deepfake pornography? To answer this, relevant provisions must first be identified.

Deepfake pornography is related to those national provisions criminalizing the distribution of intimate material that MSs have recently adopted or modified on the wave of a renewed social sensibility to the phenomenon of gender violence.¹²² The notions commonly employed here are “non-consensual pornography” and “revenge porn”. The relationship between these two on one hand, and deepfake pornography on the other, has already been introduced in this research as a complicated one.¹²³ Non-consensual pornography is alternatively described as a synonym of revenge pornography, or as a broader category, in which deepfake pornography would fall.

Recent doctrine has started to criticize the expressions “revenge porn” and “non-consensual pornography” on account of their inability to fully outline the phenomena they try to describe.¹²⁴ Both use the term “pornography”, which is misleading. First, because not all the images that are disseminated against the will of the person depicted (or taken without their consent, for instance with a hidden camera in a public restroom) are of a pornographic nature, they could simply represent them

¹²¹ Patrick Grady, ‘EU Proposals Will Fail to Curb Nonconsensual Deepfake Porn’ (*Center for Data Innovation*, 23 January 2023) <<https://datainnovation.org/2023/01/eu-proposals-will-fail-to-curb-nonconsensual-deepfake-porn/>> accessed 27 April 2024. The Croatian criminal code provides a norm that punishes deepfake pornography and will be addressed at the end of the next subsection.

¹²² This research will not address those criminal offences that may encompass deepfake pornography from other angles, such as identity theft or cyberstalking, first because they are not always applicable, and second because they shift the focus away from the dimension of gender violence. On their relationship with deepfake pornography see: Delfino (n 38) 909ff; Suslavich (n 7) 173.

¹²³ *Supra*, Chapter 1.4.

¹²⁴ In particular, McGlynn & Rackley (n 116). See also more recently Rüya Tuna Toparlak, ‘Criminalising Deep Fake Pornography - A Gender-Specific Analysis of Image-Based Sexual Abuse’ (2023) 1 *Cognitio – studentisches Forum für Recht und Gesellschaft* 1. Rigotti and McGlynn (n 34) 456, go as far as to write that the very use of the expression “revenge porn” is a key reason for the limited and myopic approach adopted in public discourse over image-based gender violence.

in an intimate context. Second, because it seems to imply the intention of sexual gratification in the author, whereas it is just one of many possible reasons.¹²⁵ Third, because it associates the term “pornography”, which in itself can be consensual, with an abusive act.¹²⁶

The expression “revenge porn”, although familiar to the public, is even more limited, in that it only points to those behaviours where the diffusion of intimate/pornographic material is done out of revenge, usually from a rejected lover or an ex-partner.¹²⁷ Although certainly not uncommon, revenge is not the only motive behind these acts. Other reasons could be the coercion of the victim to obtain monetary or sexual advantages, or intimidation, and even to push victims into the sex trade.¹²⁸ Additionally, the term “revenge” seems to suggest that the victim with his or her behaviour somehow “provoked” the diffusion of the material.¹²⁹

Because of these limitations, this doctrine prefers the expression “image-based sexual abuse” (IBSA), which has significant merits. First, it “immediately and accurately conveys the significant harms that may occur and reflects the experiences of victim-survivors. It also identifies image-based sexual abuse as a form of sexual violence, locating it within sexual offence law and policies.”¹³⁰ Furthermore, it relates easily to the notion of deepfake pornography as image-based sexual abuse by means of digitally altered content, as already suggested.¹³¹

Keeping in mind the limitations of the notions of revenge porn and non-consensual pornography compared to IBSA, these three expressions are here used interchangeably with the same broad meaning of the distribution of sexually explicit or intimate images of someone without their consent, even if the picture or video was originally taken with the knowledge or consent of the depicted person, and for any purpose.¹³²

The following subsection will take some examples from national criminal legislation to illustrate how such provisions criminalize these behaviours, regardless of the terminology employed.

3.3 Key examples from selected national legal systems¹³³

Having identified what will be searched for in national legislation, examples will now be presented. The interaction between IBSA and deepfake pornography varies according to the presence or the absence of a specific regulation, and to the different ways IBSA is punished.

Not all MSs produced a specific IBSA regulation. Among those that have not, an interesting case is **Germany**. German criminal law does not address any form of IBSA explicitly.¹³⁴ Criminal liability can be derived for revenge porn acts from Section 201a of the German Criminal Code,¹³⁵ although the provision was not created for this purpose.¹³⁶ Under paragraph 2, it is punished the act of making

¹²⁵ McGlynn and Rackley (n 116) 536.

¹²⁶ Nikolaos Z. Zeniou, ‘Criminal Law Responses to “Revenge Porn” in Cyprus and England: Identification of the Offence and the Need for Legislative Regulations and Prevention’ in Tatiana-Eleni Synodinou, Philippe Jougoux, Christiana Markou, Thalia Prastitou-Merdi (eds), *EU Internet Law in the Digital Single Market* (Springer 2021) 383.

¹²⁷ Toparlak (n 124) 4.

¹²⁸ Zeniou (n 126) 383.

¹²⁹ *ibid.*

¹³⁰ McGlynn and Rackley (n 116) 536-537. Of the same opinion: Toparlak (n 124) 4; Zeniou (n 126) 84.

¹³¹ *Supra* Chapter 2.5.

¹³² Expanding on the definition given by Chesney and Franks (n 37) 346 and by McGlynn and Rackley (n 116) 537.

¹³³ Refer to the Annex to read the full version of the articles quoted, the text in the original language, and where they can be found.

¹³⁴ Mania (n 19) 121.

¹³⁵ §201a Strafgesetzbuch, Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen (Violation of the most personal sphere of life and personal rights by taking pictures).

¹³⁶ See Mania (n 19) 121; David Ryan, ‘European remedial coherence in the regulation of non-consensual disclosures of sexual images’ (2018) 34 Computer Law Security Review 1053, 1062.

accessible to a third person, without consent, the image of another person if it is likely to significantly damage the reputation of the person depicted.¹³⁷

Section 201a StGB rests on the consideration that the depicted person's privacy is infringed by the perpetrator's act of diffusing the image/video.¹³⁸ So, even if the diffusion of deepfakes could be assimilated to the act of making available intimate material, and thus be punished under this provision, the same could not be said about its production.¹³⁹ In addition, even if Section 201a StGB included deepfakes, they would still be treated as minor privacy violations, and not as sexual offences, with consequences on the level of punishment and that of the social condemnation.¹⁴⁰

Section 201a StGB must be read together with a 2015 ruling of the German Federal Court (Bundesgerichtshof).¹⁴¹ The BGH established that, when a relationship ends, the validity of the consent given when the image/video was taken runs out, and the ex-partner must delete said material upon request.¹⁴² This implies that the very existence of intimate material without consent can be the basis for criminal liability. And, since the occasion for the BGH decisions was that the material was (a) of a sexual nature and (b) held without the consent of the depicted person, the same conclusion could, in theory, be reached about deepfake pornography.

In other legal systems, provisions have been introduced to target IBSA. In **Portugal**, victims can claim compensation or ask for a prison sentence on account of the intrusion of privacy caused by the dissemination of intimate material.¹⁴³ Therefore, even if the provision could be extended to deepfake pornography, the victim would still have to prove a violation of the right to privacy.

Most MSs present *ad hoc* IBSA criminalization forms. The **Maltese** Criminal Code punishes the act of disclosing intimate or sexual material without consent, but under condition of the "intent to cause distress, emotional harm or harm of any nature".¹⁴⁴

In **Spain**, the Criminal Code establishes criminal liability for the non-consensual dissemination of intimate material originally obtained with the consent of the depicted person.¹⁴⁵ The provision refers exclusively to (real) content originally shared with consent,¹⁴⁶ and in any case establishes only a minor privacy liability, prosecuted only in cases of serious damage to privacy.¹⁴⁷

The **Swedish** Criminal Code includes several forms of IBSA, such as "acts of intrusive photography".¹⁴⁸ Anyone infringing on someone else's privacy by spreading information about them, including images of their fully or partially naked body, can be held liable.¹⁴⁹

¹³⁷ §201a StGB, para 2.

¹³⁸ Mania (n 19) 121; Katlyn M. Brady, 'Revenge in Modern Times: The Necessity of a Federal Law Criminalizing Revenge Porn' (2017) 28 Hastings Women's LJ 3, 21-22.

¹³⁹ As proposed by Tobias Lantwin, 'Deep Fakes – Düstere Zeiten Für Den Persönlichkeitsschutz? Rechtliche Herausforderungen Und Lösungsansätze' (2019) MultiMedia Und Recht, available at <<https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2FMMR%2F2019%2Fcont%2FMMR.2019.574.1.htm>> accessed 27 April 2024. Lantwin's interpretation is picked up by European Parliamentary Research Service (n 4) 61.

¹⁴⁰ Mania (n 19) 123.

¹⁴¹ Bundesgerichtshof, 13.10.2015—VI ZR 271/14, available at <<https://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=BGH&Datum=13.10.2015&Aktenzeichen=VI%20ZR%20271%2F14>> accessed 27 April 2024. See Mania (n 19) 121.

¹⁴² Brady (n 138) 22.

¹⁴³ Portuguese Criminal Code, art 192.

¹⁴⁴ Maltese Criminal Code, art 208(E).

¹⁴⁵ Spanish Penal Code, art 197(7).

¹⁴⁶ Article 197 is titled "On discovery and revelation of secrets".

¹⁴⁷ Mania (n 19) 122.

¹⁴⁸ Swedish Criminal Code, Chapter 4, section 6a.

¹⁴⁹ Swedish Criminal Code, Chapter 4, section 6c, letter 5.

In **Slovenia**, publishing photographs or videos with sexual content of another person without that person's consent is punished only insofar as it severely affects that person's privacy.¹⁵⁰

The **Slovakian** Criminal Code punishes those who unauthorizedly disseminate material of a personal nature, under two conditions: that the material was originally obtained with the consent of the person depicted; that such dissemination is capable of significantly endangering the reputation or causing other serious damage to the rights of the victim.¹⁵¹

In **France**, the acts of taking and diffusing intimate material are criminalized as revenge porn.¹⁵² However, the images referred to in the relevant articles are real pictures, which excludes the creation as well as the dissemination of deepfake pornography from the punishable offences.¹⁵³

In **Italy**, Art. 612-ter paragraph 1 of the Criminal Code punishes the publication or sharing of sexual images, after having created or subtracted them, absent consent.¹⁵⁴ Unlike the French provision, the Italian one makes revenge porn an independent criminal offence, not linked to a privacy infringement.¹⁵⁵ However, like the French equivalent, the Italian norm was written specifically for traditional situations of revenge porn, and the wording suggests against its extension to deepfake pornography.¹⁵⁶ Art. 612-ter paragraph 2 extends the same punishment to those who, having received the material in the way described by paragraph 1, further distribute them with the intent to harm.¹⁵⁷

The **Belgian** and **Romanian** IBSA criminal provisions, like the Italian one, classify it as a form of sexual abuse, and not a privacy offence.¹⁵⁸ However, again, their wording seems well suited only to address “real” pornographic content.

Another MS where criminal legislation has recently been expanded to specifically address IBSA is the **Netherlands**. Article 139(h) of the Criminal Code punishes the intentional and unlawful

¹⁵⁰ Slovenian Criminal Code, art 143(6). Critical of the privacy infringement requirement, especially given the ambiguous way it is formulated, are Šepeč and Lango (n 17) 123. A similar provision comes from a country that is not a MS yet. The Serbian Criminal Code provides for a broad IBSA criminal provision that could be extended to deepfake pornography, but it includes the narrowing requirement of a significant violation of the private life of a person. The reference is to Article 145 Serbian Criminal Code, official translation available at <https://www.mpravde.gov.rs/files/Criminal%20%20%20Code_2019.pdf> accessed 28 April 2024. See Šepeč and Lango (n 17) 124-125.

¹⁵¹ Slovakian Criminal Code, Chapter 9, section 360b.

¹⁵² A 2016 reform modified Section 1 of the French Criminal Code (Code pénal), titled “De l’atteinte à la vie privée”, including among the offences against privacy the behaviour of taking, recording or transmitting, without the person's consent, the image of a person in a private place (Article 226-1 Code pénal, modified by Loi n°2020-936 du 30 juillet 2020 - art. 17), and the act of retaining, bringing or allowing it to be made known to the public or a third party or using in any manner whatsoever any recording or document obtained using one of the acts provided for by the previous article (Article 226-2 Code pénal, modified by Loi n°2020-936 du 30 juillet 2020 - art. 17). When object of these behaviours are sexual pictures, this constitutes a form of revenge porn, in which case penalty is increased to a maximum of two years imprisonment and a fine of €60,000 (Article 226-2-1 Code pénal, introduced by Loi n°2016-1321 du 7 octobre 2016 - art. 67).

¹⁵³ See the wording of Art. 226-1, to which the other two articles refer for the description of the conduct.

¹⁵⁴ Codice Penale, art 612-ter (1). Article 612-ter has been introduced with the modification to the Code introduced by Legge 19 luglio 2019, n. 69, so called “Codice Rosso” (Red Code).

¹⁵⁵ Mania (n 19) 123; Šepeč and Lango (n 17) 126.

¹⁵⁶ The fact that paragraph 1 refers to the creation and not only to the dissemination should not lead to the conclusion that the creation of fake intimate material is punished: textual analysis of the wording used by the legislator suggests that the criminalization falls on the dissemination subsequent to the creation or the subtraction, and not on the creation itself. Besides, the same paragraph 1 limits the criminalized conduct to pictures/video “intended to remain private”, thus excluding fake content. Against the extension see: Marco Martorana and Zakaria Sichi, ‘Deepfake e revenge porn: punti di contatto’ (2021) <<https://www.altalex.com/documents/news/2021/06/03/deepfake-e-revenge-porn-punti-di-contatto>> accessed 27 April 2024. In favour of the extension see instead: Rizzica (n 50) 22.

¹⁵⁷ Codice Penale, art 612-ter (2).

¹⁵⁸ Rigotti and McGlynn (n 34) 461. For Belgium, art 417/9 Belgian Criminal Code is included in Chapter 1/I, titled “Des infractions portant atteinte à l’intégrité sexuelle, au droit à l’autodétermination sexuelle et aux bonnes mœurs”. The Romanian provision limits its scope to image-based sexual abuse as a form of domestic violence, according to art 4(1)(h) Law no. 217 of May 22, 2003.

production of the sexual image of a person;¹⁵⁹ the possession of such image when the holder knows or should reasonably suspect that the image has been intentionally and unlawfully created;¹⁶⁰ the publishing of such image;¹⁶¹ the disclosure of a sexual image knowing that it could be detrimental to the depicted person.¹⁶² Although these provisions do not explicitly mention the creation of fake material, they refer to “production” in an intentionally broad sense.¹⁶³ Since nothing in the letter of the law seems to limit the scope to the production of non-fake images, the term could include both the behaviour of taking a picture with a camera and creating a deepnude.¹⁶⁴

Similarly to the Netherlands, **Ireland** has adopted a broad form of IBSA criminalization covering distribution, publishing, or threat to do so, of an intimate image (a) without consent and (b) with intent to cause harm or being reckless as to whether or not harm is caused.¹⁶⁵ The provision is accompanied by the clarification that “intimate image” includes any form of visual representation, including “digital representation”, of “what is, *or purports to be* the person’s genitals, buttocks or anal region and, in the case of a female, her breasts”.¹⁶⁶

Finally, **Croatia** provides an example of a MS specifically criminalizing deepfake pornography as a privacy offence. The norm extends revenge porn punishment to “[w]hoever creates a new recording of sexually explicit content or modifies the existing one, by use of a computer system or in any other way, and uses it as the authentic one, thus violating the privacy of the person in the recording”.¹⁶⁷ Deepfake pornography is described here as any form of computer-generated sexual content, created either from scratch or by modifying an existing one, which is a definition in line with the one proposed in this research.¹⁶⁸

It is also interesting to notice a potential limitation of this provision: the content must be “used as the authentic one”, implying a potentially deceiving attitude of the deepfake. This, however, would in turn entail that if the fake pornography is not realized with sophisticated tools (or it simply does not aim to deceive the viewer), this provision does not apply.

To conclude, this subsection has provided a few examples of how MSs deal with deepfake pornography in their criminal legislation. Certain legal systems do not criminalize IBSA directly. In Germany, an interpretation of deepfake pornography as a privacy-related offence is present but problematic. In other countries, IBSA is explicitly criminalized as a privacy-related offence (e.g. Spain, Malta, France) or as a form of sexual abuse (e.g. Italy, Belgium, Romania), but these provisions do not seem to marry well with non-traditional forms of revenge porn. In other legal systems (e.g. the Netherlands, Ireland) criminal provisions specifically addressing IBSA are formulated in such a way that deepfake pornography could be included. Finally, Croatia is one example of a MS criminalizing deepfake pornography.

Overall, the panorama is particularly fragmented. It seems that a dissimilar conceptualization of image-based sexual abuse results in different conducts being criminalized, and ends up in a divergent understanding of and approach to deepfake pornography.¹⁶⁹

¹⁵⁹ Dutch Criminal Code (Wetboek van Strafrecht), art 139(h)(1)(a).

¹⁶⁰ Dutch Criminal Code, art 139(h)(1)(b).

¹⁶¹ Dutch Criminal Code, art 139(h)(2)(a).

¹⁶² Dutch Criminal Code, art 139(h)(2)(b).

¹⁶³ Preparatory works of the House of Representatives support this reading by confirming the intent of the legislator to extend the reach to new forms of image-based sexual abuse. See Stevens (n 50) for an in-depth study of the Dutch legal response to deepfake pornography and the conclusion in favour of the applicability of art 139(h).

¹⁶⁴ Rigotti and McGlynn (n 34) 466.

¹⁶⁵ Harassment, Harmful Communications and Related Offences Act 2020, Number 32 of 2020, art 2.

¹⁶⁶ Harassment, Harmful Communications and Related Offences Act 2020, Number 32 of 2020, art 2, emphasis added.

¹⁶⁷ Croatian Criminal Code, art 144a para 2. For a Croatian commentary on this recent modification see <<https://www.iusinfo.hr/aktualno/u-sredistu/elektronicko-nasilje-nad-zenama-50237>>.

¹⁶⁸ *Supra*, Chapter 2.5.

¹⁶⁹ Rigotti and McGlynn (n 34) 467.

3.4 Problematic aspects of including deepfake pornography in traditional revenge porn regulation

The previous subsection illustrated a few examples of national criminal legislation (potentially) extendable to deepfake pornography. This subsection will build on the issues highlighted a theoretical and systematic approach to the limits of IBSA criminalization extension to deepfake pornography.¹⁷⁰

a. Creation vs dissemination - IBSA and deepfake pornography are similar phenomena, in that they both involve the non-consensual dissemination of sexual or intimate material.¹⁷¹ A difference lies in the circumstance that in the former case the material is only shared, in the second it must be created. As IBSA laws are focused on the *actus reus* of disseminating real material, and do not include the act of creating it, these provisions are unsuitable for fake pornography, or rather, they target only a part of it (e.g. Spain, France, Italy).

b. Identification of the victim – Unlike IBSA, deepfake pornography features two persons. One is the deepfaked, i.e. the person whose facial features are reproduced, and the other is the person whose body is used, as they normally did not give their consent.¹⁷² Instead, IBSA in its traditional form is criminalized as an offence directed to one person.¹⁷³ Thus, the extension of IBSA provisions to deepfake pornography is impaired by the impossibility of identifying a second victim, which would be excluded from the criminal proceeding.

c. Intent to cause harm – As for the *mens rea*, certain criminal codes require the intent to cause harm to the victim (for instance, the Maltese and the Italian¹⁷⁴ ones). A similar requirement, widely present also among North American statutes,¹⁷⁵ is explainable in the context of revenge porn, where between actor and victim there is generally a connection, and the diffusion of intimate material responds to a logic of “revenge”.¹⁷⁶ That is not necessarily the case for deepnudes, where the intent to cause harm is only one of the reasons.¹⁷⁷ Therefore, provisions requiring the intent to cause harm are ill-suited to address deepfake pornography: first, because many cases of deepfake pornography would fall outside its scope,¹⁷⁸ second, because intent to harm is even harder to prove than cases of traditional IBSA, given that the victim may not even know an image has been created.¹⁷⁹

d. Existence of a privacy violation – The previous subsection has brought several examples of national laws criminalizing IBSA based on privacy infringement (e.g. Portugal, Spain, Slovenia, France).¹⁸⁰ As these norms are designed to protect the intimacy of the person depicted, it follows logically that damage to privacy must be present and proven. The connection of deepfake pornography to sexual privacy, however, is not as clear, because no intimate material is technically involved. On one hand, pictures used to train the AI can be publicly available, for instance, posted on social media.¹⁸¹ On the other hand, what is divulged is not the actual intimate material, but only a

¹⁷⁰ *ibid* 461ff. Similar systematic considerations on the inadequacies of laws criminalizing revenge porn to cover deepfake pornography are well present in the North American scholarly debate, on which see for instance Delfino (n 38) 921ff.

¹⁷¹ Delfino (n 38) 896.

¹⁷² *ibid* 898. However, as noted by Šepeč and Lango (n 17) 121, usually bodies alone cannot be used to identify a certain person, a consideration that would eliminate privacy concerns regarding this second type of victim.

¹⁷³ Delfino (n 38) 922.

¹⁷⁴ Only with reference to the second paragraph of art 612 ter.

¹⁷⁵ Harris (n 25) 121.

¹⁷⁶ The discussion on the opportunity to have such a condition in IBSA provisions, especially considering the difficulty of giving the related proof, falls outside the scope of this research. See Delfino (n 38) 921.

¹⁷⁷ *Supra* Chapter 2.3.

¹⁷⁸ Nicola Henry and Asher Flynn, ‘Image-Based Sexual Abuse: Online Distribution Channels and Illicit Communities of Support’ (2019) 25 *Violence Against Women*, 1932, 1950; Harris (n 25) 121.

¹⁷⁹ Flynn and others (n 74) 1343.

¹⁸⁰ Unlike the majority of European countries, most North American states treat it as a sexual offence. Šepeč and Lango (n 17) 122.

¹⁸¹ Gieseke (n 44) 1502.

fake representation on which, it could be argued, no reasonable expectation of privacy is possible.¹⁸² Therefore, the requirement of a privacy violation as *condicio sine qua non* for punishment makes the application of those provisions to deepfake pornography unconvincing.¹⁸³

e. Intimate/Sexual material - The same conclusion can be reached even in those cases, such as Italy, where IBSA is not qualified as a privacy offence, but reference to intimate or sexual material is made: in fact, the material used to create the deepfake is not sexual (otherwise, there would be no “need” for a deepfake). Therefore, the reference to “sexually explicit content”,¹⁸⁴ or “sexual content”¹⁸⁵ limits the applicability of these provisions to deepfake pornography.¹⁸⁶

f. Consent - All IBSA criminal laws presented in the previous subsection require the absence of consent to the dissemination of intimate material.¹⁸⁷ This is an element shared by IBSA and deepfake pornography, which both require a lack of content to realize a punishable offence. Consent is lacking in IBSA by definition. Instead, the deepfaked, although usually unaware or against the use of his/her face to create the deepfake, can in theory give consent to this use of their appearances.¹⁸⁸

In addition, the nature and activities covered by consent are different. In IBSA, consent must come from the (only) victim and cover the diffusion of intimate images, whereas in deepfake pornography it should be evaluated with regard to both production and diffusion,¹⁸⁹ and must come from both victims.¹⁹⁰

3.5 Final remarks

As it emerges from the multitude of problems depicted in the previous section, the extension of IBSA criminal laws to deepfakes pornography is met with many challenges. In general, the shortcomings of these provisions are shown by their wording, which reflects the intent of national legislators to punish only traditional forms of image-based sexual abuse, hence the reference to “real” pictures/videos (e.g. France), to generic harm (e.g. Malta), or to specific harm to privacy (e.g. Slovenia).

In certain legal systems, (e.g. the Netherlands), IBSA provisions are designed in such a broad way that national courts could use them to convict deepfake pornography producers or distributors (only the latter, in the case of Ireland). But if IBSA criminal provisions are not designed in that way, as it happens for most MSs considered, then they are unfit for extension.

It can be concluded that, unless they are specifically designed to comprehend deepfake pornography, IBSA criminal laws are unsuitable for this operation. This leaves a criminal liability void in those MSs that did not enact a specific provision on deepfake pornography, such as Croatia, nor a sufficiently broad one for IBSA.

¹⁸² Delfino (n 38) 897; Harris (n 25) 121.

¹⁸³ Art 612 ter of the Italian Criminal Code is classified as a crime against personal freedom (Capo III) and more specifically against moral freedom (within Capo III, Sezione III), a choice commented favorably by Mania (n 19) 123 and Šepece and Lango (n 17) 126.

¹⁸⁴ Italian Criminal Code, art 612-ter (1).

¹⁸⁵ Belgian Criminal Code, art 417/9; Slovenian Criminal Code, art 143(6).

¹⁸⁶ As noticed by McGlynn and Rackley (n 116) 541. See Rigotti and McGlynn (n 34) 462ff, for a detailed investigation of the notions of sexual, private and intimate material from a EU perspective. See Harris (n 25) 122-123, for the debate in US literature on the possibility to interpret extensively US revenge porn statutes referencing “intimate body parts” or “sexual acts” to deepfake pornography.

¹⁸⁷ It is irrelevant to the notion of revenge pornography if consent was originally given and then ceased, or if it was never given. On consent as an element of revenge pornography see Ava Schein, ‘When Sharing is Not Caring: Creating an Effective Criminal Framework Free from Specific Intent Provisions to Better Achieve Justice for Victims of Revenge Pornography’ (2019) 40 Cardozo Law review 1953.

¹⁸⁸ Citron and Chesney (n 1) 1771; Delfino (n 38) 897.

¹⁸⁹ One could, for instance, give consent to the partner to deepfake them, without permitting to disseminate the content created.

¹⁹⁰ Delfino (n 38) 922.

CHAPTER 4 - ENTERS THE EUROPEAN UNION: OUTLINES OF A COMMON FIGHT AGAINST DEEPPAKE PORNOGRAPHY

4.1 Introduction

So far, this research has approached the analysis of deepfake pornography in a twofold way. In Chapter 2, the study of deepfake pornography as the misuse of a technology, as a social phenomenon, and as a morally objectionable behaviour, has presented some coordinates for interpreting what is meant by deepfake pornography and the boundaries of this notion, ultimately underlying the difficulties of identifying a clear definition. In Chapter 3, research has taken a more practical form. Selected instances of image-based sexual abuse criminalization in European national legislations have provided the examples necessary to identify a trend of indirect criminalization of deepfake pornography through IBSA laws (and its exceptions) and the shortcomings of this approach.

Chapter 4 starts from these premises and introduces a new player: the European Union institutions (EU). This chapter aims to clarify the role of the EU in the fight against deepfake pornography with particular regard to the new Commission Proposal on combating violence against women and domestic violence.¹⁹¹

Section 4.2 describes the political and programmatic context in which the Proposal was presented by retracing the steps that led to that decision. Ultimately, this part will make clear why the Commission decided to draft this text, why now, and why in this way. Section 4.3 will briefly sketch the legislative *iter* up until the modification introduced by the Parliament at first reading.¹⁹² The description of the content and the structure of the Proposal will contextualise the critical analysis of the provision regarding deepfake pornography (section 4.4).

As a final clarification, it should be noted that the phenomenon of deepfake pornography is already (potentially) targeted by EU non-criminal legislation. First, sharing a deepfake could constitute an unlawful processing of data according to Art. 17 GDPR,¹⁹³ allowing the deepfaked to request its erasure to the platforms where it is shared.¹⁹⁴ Second, under the Digital Services Act,¹⁹⁵ platforms

¹⁹¹ Commission, 'Proposal for a Directive of the European Parliament and of the Council 2022/0066 of 8 March 2022 on combating violence against women and domestic violence' COM/2022/105 final (Gender Violence Proposal)

¹⁹² European Parliament, 'Legislative resolution of 24 April 2024 on the proposal for a directive of the European Parliament and of the Council on combating violence against women and domestic violence' (COM(2022)0105 – C9-0058/2022 – 2022/0066(COD)) P9_TA(2024)0338.

¹⁹³ 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).

¹⁹⁴ Stevens (n 50) 28. However, as Mania (n 19) 119 notes, exercising the right to erasure is no easy task: the procedure is long and costly, and the right difficult to prove, particularly for instances of IBSA.

¹⁹⁵ 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).

must play an active (and demonstrable) role in taking down illegal material.¹⁹⁶ Third, the AI Act could deter the creation and sharing of AI-generated fake content.¹⁹⁷

Considerations related to privacy, platform regulation and regulation of AI go beyond the scope of this research. But certainly, the Gender Violence Proposal would contain the first provision directly targeting deepfake pornography as a criminal phenomenon by harmonising national criminal law (outside the area of child protection, as will be illustrated).

4.2 The EU fight against gender-based violence: from the Gender Equality Standard to the Istanbul Convention

As the EU traditionally does not use the instrument of the harmonization of criminal substantive law, it is appropriate to wonder why the Commission has chosen to propose a Directive containing such provisions. To explain this, this section retraces the role of the EU in the battle against gender-based violence.¹⁹⁸

Within the European Pillar of Social Rights, the EU has set as a key goal for the future to erase discrimination based on gender. This is made clear in the Gender Equality Strategy 2020-2025, a programmatic document in which the Commission announces its intention to implement this objective in all the areas where the EU regulates.¹⁹⁹ Among the policy objectives set out, such as addressing the gender gap in the labour market and in decision-making positions, the first one is

¹⁹⁶ See the Commission's website at <https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/digital-services-act_en> accessed 27 April 2024. However, while mainstream content-sharing websites already have in place measures to prevent the spread of non-consensual pornography (although not always with significant results, see in the news Bryan Clark, 'Pornhub promised to ban 'deepfakes' videos. And it failed miserably.' (TNW, 19 April 2018) <<https://thenextweb.com/news/pornhub-promised-to-ban-deepfakes-videos-and-it-failed-miserably>> accessed 27 April 2024) deepfakes are mostly hosted on dedicated platforms. Popova's research (n 83) found that deepfake pornography is often confined to certain internet communities. As noted by Flynn (n 74) 1343, many platforms are slow to implement these mechanisms, or they place the burden of giving proof on victims. It has been argued therefore (Grady (n 121)) that the DSA will play a limited role against non-consensual deepfakes.

¹⁹⁷ Commission, 'Proposal for a Regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts' COM (2021) 206 final. However, the Commission's concern in this regard is to avoid the spread of deceiving content, whereas, as illustrated above (Chapter 2.3) authenticity is not a typical feature of deepfake pornography, nor one requested by its viewers. Grady (n 121).

¹⁹⁸ It is necessary to clarify from the start what is meant in this context by "gender-based violence", as the expression is commonly used in EU legislation and international treaties. For instance, in the Istanbul Convention, art 3(d), it is meant as "violence that is directed against a woman because she is a woman or that affects women disproportionately". The definition is shared in EU legislation, where it is defined as "violence that is directed against a person because of that person's gender, gender identity or gender expression or that affects persons of a particular gender disproportionately", and causing "physical, sexual, emotional or psychological harm, or economic loss, to the victim". See Directive 2012/92/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA (Victims' Rights Directive), para 17. More recently, it has been shared by the Gender Violence Proposal, art 4(a). However, as the Parliament itself noted, there is an overall lack of harmonisation in MSs on the notion. See European Parliament, 'Resolution of 14 December 2021 with recommendations to the Commission on combating gender-based violence: cyberviolence (2020/2035(INL))' lett r. The problem has not been solved by the Gender Violence Proposal, which only defined violence against women, disregarding Parliament's recommendations. See European Parliamentary Research Service, Nora Hahnkamper-Vandenbulcke and Izabela Bacian, 'Violence against women and domestic violence - The new European Commission proposal in light of European Parliament requests' (2022) PE730.329 <[https://www.europarl.europa.eu/RegData/etudes/STUD/2022/730329/EPRS_STU\(2022\)730329_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/730329/EPRS_STU(2022)730329_EN.pdf)> accessed 27 April 2024, 38.

¹⁹⁹ Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A Union of Equality: Gender Equality Strategy 2020-2025' COM (2020) 152 final, 1.

“ending gender-based violence”.²⁰⁰ One of the ways the Commission plans to do so is “extending the areas of crime where harmonisation is possible to specific forms of gender-based violence”, thus recognising criminalization as one of the key actions to combat gender inequality.²⁰¹

Next to the Commission, the role of the European Parliament as an active player in the programmatic fight against gender-based violence is expressed in a series of documents.²⁰² In a 2021 Resolution, the Parliament recommends a “holistic approach”, that is to address all forms of gender-based violence, regardless of where they happen (online, offline), of their target (LGBTIQ+ persons, adult women and girls, partners and strangers), and of the nature of the harm caused (physical, sexual, economic and psychological).²⁰³ Further, the Parliament recognises the social urgency of gender-based violence,²⁰⁴ the need to prevent the crimes and support the victims with all the means necessary,²⁰⁵ and the supra-national dimension of the phenomenon, which calls for harmonisation mechanisms and common responses.²⁰⁶

In another resolution from the same year, directed at the Commission and focussing on gender-based cyberviolence, the Parliament underlines the pressing nature of online violence against women. On one hand, MSs are encouraged to adopt preventive measures (e.g. to promote awareness, digital education, and training), implement support mechanisms for victims, and provide for criminal law responses.²⁰⁷ On the other, the Commission is urged to support MSs in the adoption of said policies, and at the same time to act firsthand to criminalise gender-based cyberviolence, in view of a future harmonising effect on national legislations.²⁰⁸

Of great political and legal relevance is the recent accession of the EU to the Convention on preventing and combating violence against women and domestic violence (“Istanbul Convention” from here on).²⁰⁹ The Convention, promoted by the Council of Europe and signed in Istanbul in 2011, has been signed and ratified by most EU MSs.²¹⁰ In 2016, the Commission proposed the Council to access the Convention as a legal instrument necessary to implement gender equality and combat gender-based violence, as enshrined in the Treaties and required by the Charter of Fundamental

²⁰⁰ Gender Equality Strategy 2020-2025, 3.

²⁰¹ *ibid.* Other ways to end gender-based violence outlined are, for instance, launching an EU network on the prevention of gender-based violence and domestic violence, and encouraging MSs to ratify the International Labour Organisation (ILO).

²⁰² Besides several resolutions, the Parliament is also responsible for commissioning a comprehensive study on gender-based cyberviolence. See: European Parliamentary Research Service, ‘Combating gender-based violence: Cyber violence’ (2021) PE 662.621. Another report, widely referenced in this thesis, focused on deepfakes in general. See European Parliamentary Research Service (n 4).

²⁰³ European Parliament, ‘Resolution of 16 September 2021 with recommendations to the Commission on identifying gender-based violence as a new area of crime listed in Article 83(1) TFEU’ (2021/2035(INL)) para 1ff.

²⁰⁴ *ibid.*, para 36: the COVID-19 pandemic has further accentuated the problem.

²⁰⁵ *ibid.*, para 47ff.

²⁰⁶ *ibid.*, para 63ff.

²⁰⁷ European Parliament, ‘Resolution of 14 December 2021 with recommendations to the Commission on combating gender-based violence: cyberviolence’ (2020/2035(INL)), *passim*, in particular para 8.

²⁰⁸ *ibid.*, para 54.

²⁰⁹ Council of Europe, Convention on preventing and combating violence against women and domestic violence, 11 May 2011, ETS 210.

²¹⁰ Bulgaria, Czech Republic, Hungary, Lithuania, and Slovak Republic have signed the Convention between 2011 and 2016 but have yet to ratify it. See the website of the Council of Europe at <<https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treaty=210>> access 27 April 2024.

Rights of the European Union.²¹¹ The Council signed the Convention in 2017.²¹² Although welcoming the Council decision, the Parliament urged MSs to proceed as well to ratify the Convention.²¹³

Afterwards, the EU accession process to the Convention has remained dormant for a few years. In 2019 the Parliament, noting the delay of the Council and of some MSs in the ratification (and that other MSs were not implementing the provisions of the Convention) urged both the Council and MSs to act.²¹⁴ In June 2023, the Council ratified the EU's accession to the Istanbul Convention, which entered into force in October of the same year.²¹⁵

Although it is already quite dated in certain regards, not least because it does not contain references to virtual pornography, the Convention is still the main international law instrument on countering gender and domestic violence.²¹⁶

To conclude on the programmatic remarks, an analysis of the political direction and the documental activity of the EU institutions (Commission, European Parliament, and Council of the EU) shows that, albeit certain setbacks,²¹⁷ the clear intent to fight gender-based violence through harmonization of criminal provisions has been demonstrated at the EU level, a consideration that lays the background for the Gender Violence Proposal.

4.3 The Gender Violence Proposal and the Parliament's Legislative Resolution of 24 April 2024

In 2021, the Parliament warned the Commission about a lack of regulation against gender-based violence, and, in accordance with the procedure established in Article 225 TFEU, urged it to act.²¹⁸ The Commission's response to this call took the shape of a Proposal for the "first comprehensive legal instrument at EU level to tackle violence against women", presented in 2022.²¹⁹

²¹¹ Gender Violence Proposal, p 2.

²¹² For details on the whole procedure see <https://eur-lex.europa.eu/legal-content/EN/HIS/?uri=COM:2016:109:FIN#2016-03-04_ADG_byCOM>.

²¹³ European Parliament, 'Resolution of 12 September 2017 on the proposal for a Council decision on the conclusion, by the European Union, of the Council of Europe Convention on preventing and combating violence against women and domestic violence' (COM(2016)0109 — 2016/0062(NLE)) OJ 2018/C 337/28.

²¹⁴ European Parliament, 'Resolution of 28 November 2019 on the EU's accession to the Istanbul Convention and other measures to combat gender-based violence' (2019/2855(RSP)) (2021/C 232/08).

²¹⁵ Council Decision (EU) 2023/1075 of 1 June 2023 on the conclusion, on behalf of the European Union, of the Council of Europe Convention on preventing and combating violence against women and domestic violence with regard to institutions and public administration of the Union, and Council Decision (EU) 2023/1076 of 1 June 2023 on the conclusion, on behalf of the European Union, of the Council of Europe Convention on preventing and combating violence against women and domestic violence with regard to matters related to judicial cooperation in criminal matters, asylum and non-refoulement. See for the press release <<https://www.consilium.europa.eu/en/press/press-releases/2023/06/01/combating-violence-against-women-council-adopts-decision-about-eu-s-accession-to-istanbul-convention/>>.

²¹⁶ European Parliament, 'Resolution of 16 September 2021 with recommendations to the Commission on identifying gender-based violence as a new area of crime listed in Article 83(1) TFEU', letter AB. In any case, what the Istanbul Convention does for the EU is only provide for a minimum standard of rules, or better, to guarantee certain standards, as was clear already in Gender Equality Strategy 2020-2025, 3. However, this does not stop the EU from further harmonization.

²¹⁷ For instance, a difference in the role of consent in the definition of rape has generated a contrast among MSs. See Clothilde Goujard, 'EU countries reject making non-consensual sex a criminal offense across the bloc' (*Politico*, 9 June 2023) <<https://www.politico.eu/article/rape-europe-criminal-offense-non-consensual-sex/>> accessed 27 April 2024.

²¹⁸ European Parliament, 'Resolution of 28 November 2019 on the EU's accession to the Istanbul Convention and other measures to combat gender-based violence' (2019/2855(RSP)) (2021/C 232/08), para 19.

²¹⁹ As written on the Commission's website <https://ec.europa.eu/commission/presscorner/detail/en/ip_24_649> accessed 27 April 2024. Indeed, no specific EU legislation on any form of violence against women exists at this point, as noted by the Council. See <<https://www.consilium.europa.eu/en/policies/eu-measures-end-violence-against-women/#directive>> accessed 27 April 2024.

The Commission picked up the task of implementing the Parliament's recommendations and the Gender Equality Standard by putting forward a proposal covering violence against women and domestic violence,²²⁰ especially regarding gender-based cyber violence, meaning acts of violence permitted or facilitated by the internet that target primarily women, deepfake pornography included.²²¹

The Proposal was also necessary to align to the international standards imposed by the Istanbul Convention (and to complement it in areas where the Convention is lacking, such as cyber violence)²²² and to protect the fundamental rights enshrined in the EU Charter of Fundamental Rights.²²³

Both the Proposal and its prodromal works demonstrate the Commission's intent to build a comprehensive framework to combat gender violence.²²⁴ The complexity of the Commission's strategy against gender-based violence explains why the Proposal includes different parts.²²⁵

An element worth highlighting is that Chapter 2 is the only one containing the harmonization of criminal law.²²⁶ In this part, the Commission proposes provisions harmonising national criminal legislation regarding sexual exploitation of women and children (e.g. rape, female genital mutilation) and computer crime (e.g. cyber stalking, cyber harassment, cyber incitement to violence or hatred). The other Chapters contain other, non-criminal provisions, such as access to justice (Chapter 3),²²⁷ MSs' obligations to support victims of gender based violence and domestic abuse (Chapter 4), preventive measures (Chapter 5) and cooperation among governmental agencies and other actors (Chapter 6).

Although with various criticisms, the Parliament has expressed overall appreciation for the way its recommendations were implemented in the Proposal.²²⁸ In February 2024, the Belgian Presidency of

²²⁰ Domestic violence is also a form of violence against women, as women are mostly the victims of violence occurring in the family or domestic environments. See Gender Violence Proposal, p 1.

²²¹ Gender Violence Proposal, p 3.

²²² Gender Violence Proposal, p 3 and 7 (but keep in mind that the EU has adopted the Convention in the meantime). In any case, this should not in any way slow down MSs' accession to the Istanbul Convention.

²²³ In particular, with regard to: human dignity (art 1), the right to life (art 2), the right to integrity (art 3), the prohibition of torture and inhuman or degrading treatment (art 4), the right to private and family life (art 7), the right to personal data protection (art 8), the rights of the child (art 24), the right to freedom from discrimination, including on the grounds of sex (artt 21 and 23), the rights to social assistance and healthcare (artt 34 and 35 of the Charter), and the right to an effective remedy and a fair trial (art 47). See more in detail Gender Violence Proposal, pp 15-16.

²²⁴ See for instance the recommendations of the Advisory Committee on Equal Opportunities for Women and Men. Advisory Committee on Equal Opportunities for Women and Men, 'Opinion on the prevention of gender-based violence and domestic violence' (2023) <https://commission.europa.eu/document/download/6391f8eb-5d1d-4646-a014-d836d0f3346d_en?filename=Opinion%20violence%20adopted.pdf&prefLang=it>.

²²⁵ See Gender Violence Proposal, pp 17-19 for a detailed explanation of its structure.

²²⁶ To anticipate a potential critique of the point of view adopted by the author, that of substantive criminal law, it is not implied here that criminal law is the only or even the primary way in which the EU intends to fight gender-based violence. In fact, even in those documents where harmonization of national criminal law is presented as an essential component of the EU gender-violence policy, other (non-legal or legal but non-penal) interventions are prospected as equally necessary, such as education in schools, functioning assistance mechanisms for victims, and law enforcement training. European Parliament, 'Resolution of 16 September 2021 with recommendations to the Commission on identifying gender-based violence as a new area of crime listed in Article 83(1) TFEU', para 68. What this demonstrates, however, is that gender-based violence is a complex sociological phenomenon that must be tackled with different, coordinated interventions. However, it is undeniable that the harmonisation of criminal law is not only a part of the EU strategy to fight gender-based violence, but actually one of the key actions.

²²⁷ As stated in Gender Violence Proposal, p 18, Chapter 3 shall be intended complementary to Directive 2012/29/EU establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA. The Directive is interesting for this research also because the provisions directed at providing a special procedural treatment of victims of gender-based violence and sexual violence, such as ensuring victims' support services (art 9) or assessing specific protection needs (art 22), could be extended to victims of deepfake pornography.

²²⁸ European Parliamentary Research Service, Hahnkamper-Vandenbulcke and Bacian (n 198).

the Council and the Parliament reached a political agreement on the Proposal.²²⁹ This agreement upheld the Commission's Proposal with regard to many key elements, such as the non-consensual sharing of pornography and deepfakes.²³⁰

After the stage of interinstitutional negotiations, the text reached the Parliament's plenary sitting in April 2024.²³¹ In the resulting legislative resolution, the text is modified, but the structure and the overall content are left unchanged.²³² For instance, the harmonization of the crime of rape was removed from Chapter 2, where the crime of forced marriage appeared instead.²³³

These modifications are, in any case, precarious. According to the ordinary legislative procedure, the Council will have to approve the same text at the first hearing. Possible modifications will be discussed by the Parliament at a second hearing.

4.4 Article 7(b): the Commission's plan to harmonize deepfake pornography criminalization

4.4.1 The content of Article 7 before and after the Parliament's Legislative Resolution: image-based sexual abuse and deepfake pornography

In 2021, the Parliament recognised that IBSA constitutes "an extreme violation of privacy and also [...] a form of gender-based violence" and urged MSs to criminalize it explicitly and in a way unrelated to child sexual abuse.²³⁴ The Commission implemented this approach in Article 7 of the Proposal, titled "Non-consensual sharing of intimate or manipulated material", which was later transposed in Article 5 of the Legislative Resolution. The two versions read:

Article 7 Proposal <i>Member States shall ensure that the following intentional conduct is punishable as a criminal offence:</i> <i>(a) making intimate images, or videos or other material depicting sexual activities, of another person without that person's consent accessible to a multitude of end-users by means of information and communication technologies;</i>	Article 5 Legislative resolution <i>Member States shall ensure that the following intentional conduct is punishable as a criminal offence:</i> <i>(a) making accessible to the public, by means of information and communication technologies ('ICT'), images, videos or similar material depicting sexually explicit activities or the intimate parts of a person, without that person's consent, where such conduct is likely to cause serious harm to that person;</i>
--	--

²²⁹ See the press release at <<https://www.consilium.europa.eu/en/press/press-releases/2024/02/06/violence-against-women-council-and-european-parliament-reach-deal-on-eu-law/>>.

²³⁰ As reported by the Commission (<https://ec.europa.eu/commission/presscorner/detail/en/ip_24_649>). Consent was not reached on other, important points of the Proposal, such as the criminalization of rape based on lack of consent as proposed by the Commission.

²³¹ See the Parliament's website at <[https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2022/0066\(COD\)&l=en](https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2022/0066(COD)&l=en)> accessed 27 April 2024.

²³² European Parliament, 'Legislative resolution of 24 April 2024 on the proposal for a directive of the European Parliament and of the Council on combating violence against women and domestic violence' (COM(2022)0105 – C9-0058/2022 – 2022/0066(COD)) P9_TA(2024)0338.

²³³ *ibid*, art 4.

²³⁴ European Parliament, 'Resolution of 14 December 2021 with recommendations to the Commission on combating gender-based violence: cyberviolence (2020/2035(INL))', para 17.

The way Article 7 Proposal is written would help overcome some of the problems of IBSA criminalization identified above²³⁵ and force MSs to update their approach to non-consensual pornography. First, it refers not only to “sexual activities”, but also to “intimate” content, covering situations, such as upskirting and downblousing, that are currently left out from certain legal systems.²³⁶ Second, it does not mention the intention to cause harm, nor any other unnecessary element related to the *mens rea*.²³⁷

The text approved by the Parliament modifies the wording in a way that nullifies said improvements. Reference to intimate images disappears, and the likelihood to cause serious harm to the person is introduced. This last requirement, besides adding an element difficult to prove in court, seems also unnecessary. Think, for instance, about the conduct of uploading a sexually explicit video of an ex-partner; the likelihood of causing serious harm does not seem to play a significant role in evaluating the disvalue of the conduct.

Modifications aside, the provision has still the merit to recognise the role of communication technologies in making available non-consensual pornography to a large number of users.²³⁸ This helps frame the problem of IBSA as a matter of technology regulation, which could lead the way to other interventions, targeting for instance the role of platforms in the matter.

Next to the provision on IBSA, the Commission, with a choice upheld by the Parliament, added a second letter designed to account for deepfake pornography.²³⁹ The wording of the text is as follows:

Article 7 Proposal <i>(b) producing or manipulating and subsequently making accessible to a multitude of end-users, by means of information and communication technologies, images, videos or other material, making it appear as though another person is engaged in sexual activities, without that person's consent;</i>	Article 5 Legislative resolution <i>(b) producing, manipulating or altering and subsequently making accessible to the public, by means of ICT, images, videos or similar material making it appear as though a person is engaged in sexually explicit activities, without that person's consent, where such conduct is likely to cause serious harm to that person;</i>
---	--

The Commission's choice to approach deepfake pornography in these terms and right after IBSA reflects an approach already suggested in the Parliament's 2021 Resolution, where deepfakes are presented as a new form of IBSA that consists of “harnessing artificial intelligence to exploit, humiliate and harass women”.²⁴⁰

The intent of the Commission to harmonise the criminalisation of deepfake pornography as a form of sexual abuse can theoretically remedy the absence of protection present in MSs due to the lack of sanctioning rules dedicated to deepfake pornography or at least to forms of IBSA other than classic revenge porn. Nevertheless, the way the provision is written (especially in the version proposed by the Parliament) and in general the way the Commission has treated deepfake pornography pose serious problems, which will be discussed in the next two sections.

²³⁵ *Supra*, Chapter 3.4.

²³⁶ Rigotti and McGlynn (n 34) 472.

²³⁷ *ibid.*

²³⁸ Gender Violence Proposal, recital 18.

²³⁹ *ibid.*, recital 19.

²⁴⁰ European Parliament, ‘Resolution of 14 December 2021 with recommendations to the Commission on combating gender-based violence: cyberviolence (2020/2035(INL))’, lett. T.

4.4.2 Problems of deepfake pornography harmonization

This and the next subsections discuss the problems with the Commission's plan to harmonize deepfake pornography criminalization. Alongside the legal basis problem that will be described in the next subsection, which generally concerns how Chapter 2 of the Directive has been designed, other issues affect the harmonisation of deepfake pornography (in itself or indirectly as a form of IBSA).

a. Multitude of end-users/the public - Article 7(b) Proposal and Article 5(b) Legislative Resolution require respectively the material to be made accessible “to a multitude of end-users by means of information and communication technologies” and “to the public, by means of information and communication technologies (‘ICT’)”. The attention to the amplifying effect of communication technologies, without which phenomena like deepfake pornography would not even exist, is certainly positive. However, the accessibility requirement seems to unreasonably limit the scope of the provision for two reasons.

First, because it introduces an element of uncertainty. How many users constitute a multitude? The Commission's clarification of “significant number of end-users” does not provide further explanation.²⁴¹ The same goes for the Parliament's clarification of “accessible to the public” as “potentially reaching a number of persons” and “having regard to the relevant circumstances, including the technology used to make that material accessible.”²⁴² Second, because the harm is not proportional to the number of end-users reached (think about intimate material shared with the family or the employer of the victim).²⁴³

b. Sexual activity/sexually explicit activities – Another critical limitation noticed by the doctrine regards the reference to the content of the fake material. Article 7(b) introduces an element of uncertainty by requesting the engagement in “sexual activities”, as no clear definition of what constitutes said activities can be provided.²⁴⁴ Besides, if a literal interpretation of the expression was to be provided, intimate non-sexual material, such as fake up-skirting or down-blousing, would be excluded.²⁴⁵ The Commission has clarified the intent to cover in the Proposal also “sexualized images”,²⁴⁶ an expression that could include intimate non-sexual material where the person depicted is seen in “sexual terms” or “to make someone or something sexually exciting”.²⁴⁷

However, the Parliament's position appears to go in the opposite direction. By changing the reference to “sexually explicit activities” in Article 5(b) of the Legislative Resolution, it seems to narrow the scope to purely pornographic content, such as a porn video or nude image.

c. Penalty – According to Article 12(6) Proposal/Article 10(4) Legislative Resolution, MSs must not set the maximum penalty for IBSA below 1 year of imprisonment. Taking into account the harm they cause, this threshold has been considered too low by the EESC, especially considering those established for similar offences, such as cyber stalking and cyber incitement to violence or hatred.²⁴⁸

d. Authenticity - Clarifying the interpretation of Article 7(b), the Commission writes that “such production or manipulation should include the fabrication of ‘deepfakes’, where the material appreciably resembles an existing person, objects, places or other entities or events, depicting sexual

²⁴¹ Gender Violence Proposal, recital 18.

²⁴² Legislative resolution of 24 April 2024, recital 18.

²⁴³ European Economic and Social Committee, ‘Opinion on the Proposal for a Directive of the European Parliament and of the Council on combating violence against women and domestic violence’ [COM(2022) 105 final] SOC/726 (2022), 3.17; Grady (n 121).

²⁴⁴ Rigotti and McGlynn (n 34) 473.

²⁴⁵ Grady (n 121).

²⁴⁶ Gender Violence Proposal, recital 19. The same text in Legislative resolution of 24 April 2024, recital 19.

²⁴⁷ Cambridge dictionary, term “sexualize”

<<https://dictionary.cambridge.org/dictionary/english/sexualize?q=sexualised>> accessed 27 April 2024.

²⁴⁸ European Economic and Social Committee, ‘Opinion on the Proposal for a Directive of the European Parliament and of the Council on combating violence against women and domestic violence’ [COM(2022) 105 final] SOC/726 (2022), para 3.18.

activities of another person, and would *falsely appear to others to be authentic or truthful*.²⁴⁹ This would exclude situations of poorly realised material, where it is clear that the porn is fake. However, as already illustrated, and as proven by the fact that users are often informed of the non-authenticity of the content, deepfake pornography is not a matter of deception.

e. Likelihood to cause serious harm – With wording similar to that of the previous letter, Article 5(b) of the Legislative Resolution requires the dissemination of deepnudes to be limited to cases where it is likely to cause serious harm to the person depicted. The requirement introduces a further (and complex) element to prove in court. Moreover, according to the Parliament, “likelihood of causing serious harm can be inferred from objective factual circumstances” and “the specific circumstances of the case should be taken into account”,²⁵⁰ which calls for extremely individualised evaluations.

4.4.3 The legal basis problem

The legal basis for Chapter 2 is Article 83(1) TFEU.²⁵¹ The intent to use this basis for such purpose was already expressed in the Gender Equality Strategy 2020-2025.²⁵² According to Article 83(1), the Parliament and the Council can establish minimum rules concerning the definition of criminal offences and sanctions, provided that the following conditions are satisfied:

- I. They have a cross border dimension, resulting from (either):
 - a. The nature of the offences;
 - b. The impact of the offences;
 - c. Or a special need to combat them on a common basis.
- II. They fit in one of the areas of particularly serious crime listed in the second subparagraph (so-called “euro-crimes”).

While rape and female genital mutilation fall within the euro-crime “sexual exploitation of women and children”, Article 7(b) and the other provisions of Chapter 2 are treated as “computer crime” offences.²⁵³

The cross-border dimension of deepfake pornography can be derived precisely from the nature of computer crime, and in particular from the possibility that perpetrators and victims do not live in the same MS.²⁵⁴ In general, when information and communication technologies are involved, as it is the case for deepfake pornography, harm is extended far beyond national borders. This creates a common problem, hence the need for common action.²⁵⁵

The duality of legal bases used by the Commission for Chapter 2 poses a problem. Rape and female genital mutilation are harmonised only with regard to female victims, because the legal basis is “sexual exploitation of women”. However, other, less harmful behaviours, such as deepfake pornography, are covered by a “gender-neutral” legal basis (computer crimes), and so they extend also to men and non-binary people. Granted that the almost totality of victims of gender-based

²⁴⁹ Gender Violence Proposal, recital 19, emphasis added

²⁵⁰ Legislative resolution of 24 April 2024, recital 18.

²⁵¹ European Parliament, ‘List of legal bases providing for the ordinary legislative procedure in the Treaty of Lisbon’ available at <https://www.europarl.europa.eu/cmsdata/198025/List_of_legal_bases.pdf> accessed 27 April 2024.

²⁵² Gender Equality Strategy 2020-2025, 3.

²⁵³ Gender Violence Proposal, pp 8-9.

²⁵⁴ European Parliament, ‘Resolution of 16 September 2021 with recommendations to the Commission on identifying gender-based violence as a new area of crime listed in Article 83(1) TFEU’ (2021/2035(INL)), para 35.

²⁵⁵ Rigotti and McGlynn (n 34) 470. Additionally, as a form of violence against women, it is also a cost for the Union, as it imposes financial burdens on States and victims as much as other euro-crimes. European Parliament, ‘Resolution of 16 September 2021 with recommendations to the Commission on identifying gender-based violence as a new area of crime listed in Article 83(1) TFEU’ (2021/2035(INL)), para 13.

violence are women, still, this kind of harmonization would introduce a double standard: while computer crimes against a male or a non-binary person are harmonized, rape perpetrated on the same victims, although certainly a more harmful crime, is not.

Moreover, as a consequence of the legal basis duality, deepfake pornography would be criminalized as a form of computer crime, which constitutes a significant matter of perspective: to treat deepfake pornography as a computer crime, to the likes of phishing or fraud, and not as a form of gender-based abuse, is a limited point of view, because it risks underestimating the role of deepfake pornography as sexual abuse, and to prevent its association with other online and offline forms of sexual abuse.

Hard as it is to establish a causal link, some of the problems described in section 4.4.2 may be linked to the narrowness of this framing. For instance, the requirement of using information and communication technologies to make the deepnude available to a multitude of end-users/to the public, or the requirement that the deepfake must be deceiving, may be due to the harmonization of deepfake pornography criminalization as a computer crime and not as a form of gender violence. However, lack of research on the Proposal precludes further considerations, and invites deeper analysis on the consequences of the Commission's approach to deepfake pornography.

However, the limits of Article 83(1) TFEU to sustain the Commission's Proposal are visible. This is also supported by the fact that the Parliament²⁵⁶ and the EESC²⁵⁷ have recommended the Commission to base its normative intervention on a new area of particularly serious crime to be identified by the Council in accordance with Article 83(1) third subparagraph.²⁵⁸ The Commission has expressed support for the introduction of a new euro-crime²⁵⁹, but it decided not to wait for it to propose the Directive regardless of the Parliament's recommendations.²⁶⁰

4.4.4 Threatening, inciting, aiding and abetting

Article 7(c) Proposal and Article 5(c) Legislative Resolution read:

(c) threatening to engage in the conduct referred to in points (a) and (b) in order to coerce another person to do, acquiesce or refrain from a certain act.

This provision would introduce an interesting novelty in national jurisdictions. The non-consensual sharing of real and fake pornography is often part of a broad scheme of acts and abuses intended to realize a position of power over the victim. As the Commission puts it, the protection offered by letters (a) and (b) would not be "effective" without covering the threat to engage in those behaviours.²⁶¹ In this sense, the fact that the use of such material in situations such as sexual extortion and blackmail, would be covered by the Directive is certainly welcome.²⁶² A limit of the way the provision is written, however, is to require the intent to coerce. First, because it is an element not always immediately clear nor easy to prove. Second, because coercive intent is not the only motivation behind real and fake IBSA (e.g. to cause distress to the victim).²⁶³

²⁵⁶ European Parliament, 'Resolution of 16 September 2021 with recommendations to the Commission on identifying gender-based violence as a new area of crime listed in Article 83(1) TFEU' (2021/2035(INL)), para 67. Already in 2019: European Parliament, 'Resolution of 28 November 2019 on the EU's accession to the Istanbul Convention and other measures to combat gender-based violence' (2019/2855(RSP)), para 20.

²⁵⁷ European Economic and Social Committee, 'Opinion on the Proposal for a Directive of the European Parliament and of the Council on combating violence against women and domestic violence' [COM(2022) 105 final] SOC/726 (2022), paras 1.5 e 3.3.

²⁵⁸ See Steve Peers, 'Substantive Criminal Law' in Steve Peers (ed), *EU Justice and Home Affairs Law: Volume II: EU Criminal Law, Policing, and Civil Law* (Oxford 2023), 211ff, on the procedure to identify a new area.

²⁵⁹ Gender Equality Strategy 2020-2025, 3.

²⁶⁰ European Parliamentary Research Service, Hahnkamper-Vandenbulcke and Bacian (n 200) 22.

²⁶¹ Gender Violence Proposal, recital 19.

²⁶² For instance, by Rigotti and McGlynn (n 34) 475.

²⁶³ *ibid.*

Other provisions of the Proposal apply to the deepfake pornography provision. Incitement, aiding and abetting (but not attempting) to share real or fake pornography shall be criminalised according to Article 11 Proposal/Article 9 Legislative Resolution.

Finally, Article 25 Proposal would force MSs to “take the necessary measures to ensure the prompt removal of material referred to in Article 7, points (a) and (b)” including the “possibility for their competent judicial authorities to issue, upon application by the victim, binding legal orders to remove or disable access to such material addressed to relevant providers of intermediary services.” Paragraph 2 clarifies that these orders can be issued also before the conclusion of the trial. According to the Parliament’s version (Article 23(1)) it is sufficient that the access to the content is disabled.

4.4.5 Coordination with other European provisions

The EU has recognised fake pornography as a criminally relevant phenomenon in relation to child pornography. Fake child pornography is a profile to which legal²⁶⁴ and ethical²⁶⁵ research has granted particular attention.

Anticipating the Cybercrime Convention, where the occurrence of technology-crafted child pornographic material is contemplated,²⁶⁶ in 2000 the Council had highlighted the need to follow closely technological developments in order to ensure the efficiency of the fight against child pornography.²⁶⁷ In 2004, the Council published a Framework Decision²⁶⁸ where the intention to target realistic pornographic images of non-existing children is made clear.²⁶⁹ The Decision was replaced in 2011 by the Directive on child pornography, which imposed that criminal provisions regarding child pornography should also encompass “realistic images of a child”.²⁷⁰

Recently, the Commission has decided to update the EU framework on child pornography by proposing a new Regulation laying down rules to prevent and combat child sexual abuse,²⁷¹ and to

²⁶⁴ For a European perspective (to be updated in light of normative interventions) see Małgorzata Skórzewska-Amberg, ‘Pornography in Cyberspace - European Regulations’ (2011) 5 Masaryk University Journal of Law and Technology 261. For US literature see for instance Rikki Solowey, ‘A Question of Equivalence: Expanding the Definition of Child Pornography to Encompass “Virtual” Computer-Generated Images’ (2002) 4 Tulane Journal of Technology & Intellectual Property 161. In that legal system, the problem is often framed in terms of balancing the protection of free speech guaranteed by the First Amendment with the harms caused to the child. See for such approach: Stacey Steinberg, ‘Changing Faces: Morphed Child Pornography Images and the First Amendment’ (2019) 68 Emory Law Journal 909.

²⁶⁵ See Eneman, Gillespie and Stahl (n 96).

²⁶⁶ Council of Europe, Convention on Cybercrime, 23 November 2001. According to art 9(2)(c), “realistic images representing a minor engaged in sexually explicit conduct” shall be considered child pornography.

²⁶⁷ Council Decision of 29 May 2000 to combat child pornography on the Internet. Art 4 reads: “Member States shall regularly verify whether technological developments require, in order to maintain the efficiency of the fight against child pornography on the Internet, changes to criminal procedural law, while respecting the fundamental principles thereof and, where necessary, shall initiate appropriate new legislation to that end.”

²⁶⁸ Council Framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography.

²⁶⁹ Council Framework Decision 2004/68/JHA, art 1(b)(iii). The Council’s Decision was particularly broad, also encompassing the possession and the production of fake child pornography, according to art 3(1)(a)-(d). However, the reach of this provision needs to be scaled down by the possibility for MSs to either exclude criminal liability in cases of mere possession of fake child pornography, or exclude its criminalisation altogether. See respectively art 3(2)(c) and art 5(4). See in literature: Skórzewska-Amberg (n 264).

²⁷⁰ Directive 2011/92/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, art 2(c)(iv).

²⁷¹ Commission, ‘Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse’ COM(2022) 209 final.

complement it with a recast of the 2011 Directive.²⁷² The latter in particular has the explicit goal to take into consideration changes in technology and the creation of deepfakes.²⁷³

This update would define a clear criminal liability for child deepfake pornography next to the one, more general, established by Article 7(b). Therefore, in this regard, the 2011 Recast Directive would constitute a *lex specialis*.²⁷⁴

Another legal text with which Article 7(b) will need to be coordinated is outside the criminal justice area. In the Digital Services Act, due diligence obligations for platforms are based on the concept of “illegal content”. Deepfake pornography is not defined (yet) as such anywhere in EU legislation, except in relation to child abuse. Article 7(b) of the Gender Violence Proposal, could fill this gap by sanctioning the illegal nature of deepfake pornography.²⁷⁵

²⁷² Commission, ‘Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child sexual abuse material and replacing Council Framework Decision 2004/68/JHA (recast)’ COM(2024) 60 final.

²⁷³ Ibid 10.

²⁷⁴ It is worth noting that Article 45 of the Gender Violence Proposal does indeed amend Directive 2011/93/EU, but not with regard to fake child pornography.

²⁷⁵ See Gender Violence Proposal, p 7. A norm that would force content-sharing pornographic platforms to provide a quick take-down procedure for content depicting a person without their consent was originally present in the DSA (art 24b) but has been discarded during the negotiations. See the discarded provision at:

<https://www.europarl.europa.eu/meetdocs/2014_2019/plmrep/COMMITTEES/IMCO/DV/2021/12-13/DSACA9_EN.pdf>. See on the choice of the Parliament to exclude this provision from the final draft: Morgan Meaker, ‘Europe Has Traded Away Its Online Porn Law’ (*Wired UK*, 27 April 2022)

<<https://www.wired.co.uk/article/digital-services-act-deepfake-porn>> accessed 27 April 2024. For a comment on how the norm would have helped in the fight against image-based sexual abuse, see: Lorna Woods and Clare McGlynn, ‘Pornography platforms, the EU Digital Services Act and Image-Based Sexual Abuse’ (*Media@LSE blog*, 26 January 2022) <<https://blogs.lse.ac.uk/medialse/2022/01/26/pornography-platforms-the-eu-digital-services-act-and-image-based-sexual-abuse/>> accessed 27 April 2024.

CHAPTER 5 – CONCLUSIONS

5.1 Answer to the research question

In this final Chapter, conclusions are drawn on the research question. Subsequently, final considerations on the limitations of the work and future research directions are provided.

At the beginning of this thesis, the research question was set in these terms: "Can the European Union's response to deepfake pornography make up for the absence of criminal liability in Member States?". Chapter 2 clarified the notion of deepfake pornography (by illustrating the characteristics of the technology, the social phenomenon, and its ethical relevance) as a form of image-based sexual abuse encompassing all forms of entirely fake or partly modified material. The analysis conducted in Chapter 3 revealed that most MS' jurisdictions present forms of criminalization of image-based sexual abuse unsuitable for extension to deepfake pornography, so that a general lack of criminalization can be seen.

Chapter 4 considered the EU response to deepfake pornography in the Directive on violence against women and domestic violence, and highlighted how its features and problems can be reflected on its harmonization effectiveness. If indeed the provision on deepfake pornography was enacted in the way it was modified by the Parliament, most MSs would have to change their criminal codes (by either modifying their IBSA provisions to guarantee extension to deepfake pornography or introducing specific norms targeting deepfake pornography). Harmonization, however, would be met with the problems described in 4.4.2 and 4.4.3.

On one hand, Article 7(b) Proposal/Article 5(b) Legislative Resolution contain unclear requirements, those of "multitude of end users"/"the public", and of "sexual activity"/"sexually explicit activity". They also assign a penalty too low compared to other crimes, and frames incorrectly deepfake pornography as a matter of content authenticity and not of sexual abuse. On the other hand, the harmonising effect could be limited by the legal basis problem. As described, according to the current formulation, national legislators are required to criminalise rape only against females, but computer crimes (such as deepfake pornography) also against men and non-binary.

So, true as it is that the Proposal would introduce in many national criminal legislations a phenomenon that otherwise would have remained outside, its several problems risk impairing an already delicate harmonization effort. In this sense, the current Commission's plan to tackle deepfake pornography makes up for the absence of criminal liability in MSs in a rather limited way.

5.2 Limitations of the work and further research

The remarks made in Chapter 4 suffer from the lack of scholarship on the Gender Violence Proposal, possibly due to the fact that it is recent and that it does not seem to have attracted much scholarly attention. Moreover, they are preliminary, as demonstrated by the Parliament's Legislative Resolution, so one must recognize the limitations of dealing with such a rule. Perhaps the Council's first reading will remedy the problems we have identified, or others that we have not paid attention to. It may also be that, as requested by Parliament, the Council will extend the legal basis, so that the Article 83(1) TFEU problem will fall in, and a solid basis will be provided.

Regardless of what will be the changes in the text, further research will be needed especially on the profile of the implementation of the harmonization process. Harmonization of substantive criminal law, even limited to the definition of offences and penalties, always comes with challenges, as criminal law is strictly linked to a society's perception of what is wrong and what should be punished, and penal provisions are part of a broad and interconnected *corpus* of norms. Some even argue that

for these reasons EU harmonization in the area of substantive criminal law cannot even reach the desired goals.²⁷⁶

Granted that certain harmonization problems may be unavoidable, when the Commission does pursue harmonization of substantive criminal law it should at least do so on a strong legal basis and with a clear understanding of the regulated phenomenon. Both these elements are not present in the Proposal, and the Parliament's modifications make for an even less effective harmonisation.

Keeping in mind that the Proposal is recent, that doctrinal reflection on the point is scarce, and that no relevant case law is known to the author, the attempt to provide a comment on the Commission's attempt to criminalize deepfake pornography is certainly impaired. However, if the Proposal was based on a legal basis directly targeting gender-based violence, which is something on which in theory both the Parliament and the Commission agree (although ultimately it is a Council decision), harmonisation could be more easily accepted and implemented in national jurisdictions. Until then, the EU's intervention should perhaps be focussed on areas where its competence to regulate is undebated, such as platform regulation and data protection.

Word count: 12645

²⁷⁶ See Satzger, 'The Harmonisation of Criminal Sanctions in the European Union' (n 55).

BIBLIOGRAPHY

Advisory Committee on Equal Opportunities for Women and Men, 'Opinion on the prevention of gender-based violence and domestic violence' (2023)

<https://commission.europa.eu/document/download/6391f8eb-5d1d-4646-a014-d836d0f3346d_en?filename=Opinion%20violence%20adopted.pdf&prefLang=it>

Ajder H, Patrini G, Cavalli F & Cullen L, 'The State of Deepfakes: Landscape, Threats, and Impact' (2019) <https://regmedia.co.uk/2019/10/08/deepfake_report.pdf>

Akdeniz Y, *Internet Child Pornography and the Law: National and International Responses* (Milton: Taylor & Francis Group 2008) 4

Bailey J and others, 'AI and Technology-Facilitated Violence and Abuse', *Artificial Intelligence and the Law in Canada* Florian Martin-Bariteau & Teresa Scassa eds (Toronto: LexisNexis Canada 2021).

Bertuzzi L, 'OECD updates definition of Artificial Intelligence "to inform EU's AI Act"' (*Euractiv*, 14 November 2023) <<https://www.euractiv.com/section/artificial-intelligence/news/oecd-updates-definition-of-artificial-intelligence-to-inform-eus-ai-act/>>

Botha J and Pieterse H, 'Fake News and Deepfakes: A Dangerous Threat for 21st Century Information Security' (15t International Conference on Cyber Warfare and Security, Old Dominion University, Norfolk, USA, March 2020)

Brady KM, 'Revenge in Modern Times: The Necessity of a Federal Law Criminalizing Revenge Porn' (2017) 28 *Hastings Women's LJ* 3

Citron DK, 'Sexual Privacy' (2019) 128 *Yale Law Journal* 1870

---- and Chesney R, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 *California Law Review* 1753

---- and Franks MA, 'Criminalizing Revenge Porn' (2014) 49 *Wake Forest Law Review* 34

Clark B, 'Pornhub promised to ban 'deepfakes' videos. And it failed miserably.' (*TNW*, 19 April 2018) <<https://thenextweb.com/news/pornhub-promised-to-ban-deepfakes-videos-and-it-failed-miserably>>

Cole S, 'AI-Assisted Fake Porn Is Here and We're All Fucked' (*Vice*, 11 December 2017)

<<https://www.vice.com/en/article/gydydm/gal-gadot-fake-ai-porn>>

---- "'You Feel So Violated": Streamer QTCinderella Is Speaking Out Against Deepfake Porn Harassment' (*Vice*, 13 February 2023) <<https://www.vice.com/en/article/z34pq3/deepfake-qtcinderella-atriloc>>

Commission, 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A Union of Equality: Gender Equality Strategy 2020-2025' COM (2020) 152 final

---- 'Proposal for a Regulation of the European Parliament and of the Council on laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts' COM (2021) 206 final

- ‘Proposal for a Directive of the European Parliament and of the Council 2022/0066 of 8 March 2022 on combating violence against women and domestic violence’ COM/2022/105 final
- ‘Proposal for a Regulation of the European Parliament and of the Council laying down rules to prevent and combat child sexual abuse’ COM(2022) 209 final
- ‘Proposal for a Directive of the European Parliament and of the Council on combating the sexual abuse and sexual exploitation of children and child sexual abuse material and replacing Council Framework Decision 2004/68/JHA (recast)’ COM(2024) 60 final
- Corstens G and Pradel J, *European Criminal Law* (Kluwer Law International 2002)
- Csonka P and Landwehr O, ‘10 Years after Lisbon – How “Lisbonised” is the Substantive Criminal Law in the EU?’ (2019) 4 *Eucrim* 261
- de Ruiter A, ‘The Distinct Wrong of Deepfakes’ (2021) 34 *Philosophy & Technology* 1311
- De Vido S and Sosa L, *Criminalisation of gender-based violence against women in European States, including ICT-facilitated violence* (Publications Office of the European Union 2021)
- Delfino R, ‘Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn’s Next Tragic Act’ (2019) 88 *Fordham Law Review* 88
- Di Noto A, ‘Mettono online video porno fake col volto di Meloni, a processo padre e figlio. La premier chiede 100mila euro: «Andranno in beneficenza»’ (*Open*, 24 October 2023)
<<https://www.open.online/2023/10/24/sassari-deepfake-meloni-processo-richiesta-risarcimento/>>
- Donegan M, ‘Demand for deepfake pornography is exploding. We aren’t ready for this assault on consent’ (*The Guardian*, 13 March 2023)
<<https://www.theguardian.com/commentisfree/2023/mar/13/deepfake-pornography-explosion>>
- Eneman M, Gillespie AA and Stahl BC, ‘Criminalising fantasies: the regulation of virtual child pornography’ (2009)
<https://www.researchgate.net/publication/265357703_CRIMINALISING_FANTASIES_THE_REGULATION_OF_VIRTUAL_CHILD_PORNOGRAPHY>
- European Economic and Social Committee, ‘Opinion on the Proposal for a Directive of the European Parliament and of the Council on combating violence against women and domestic violence’ [COM(2022) 105 final] SOC/726 (2022) <<https://www.eesc.europa.eu/en/our-work/opinions-information-reports/opinions/combating-violence-against-women>>
- European Parliament, ‘Resolution of 12 September 2017 on the proposal for a Council decision on the conclusion, by the European Union, of the Council of Europe Convention on preventing and combating violence against women and domestic violence (COM(2016)0109 — 2016/0062(NLE))’
<<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017IP0329>>
- ‘Resolution of 28 November 2019 on the EU’s accession to the Istanbul Convention and other measures to combat gender-based violence (2019/2855(RSP))’ <<https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:C:2021:232:FULL>>
- ‘Resolution of 16 September 2021 with recommendations to the Commission on identifying gender-based violence as a new area of crime listed in Article 83(1) TFEU (2021/2035(INL))’
<https://www.europarl.europa.eu/doceo/document/TA-9-2021-0388_EN.html>
- ‘Resolution of 14 December 2021 with recommendations to the Commission on combating gender-based violence: cyberviolence (2020/2035(INL))’
<https://www.europarl.europa.eu/doceo/document/TA-9-2021-0489_EN.html>
- ‘Legislative resolution of 24 April 2024 on the proposal for a directive of the European

Parliament and of the Council on combating violence against women and domestic violence' (COM(2022)0105 – C9-0058/2022 – 2022/0066(COD)) P9_TA(2024)0338

European Parliamentary Research Service, 'Combating gender-based violence: Cyber violence' (2021) PE 662.621

<[https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662621/EPRS_STU\(2021\)662621_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662621/EPRS_STU(2021)662621_EN.pdf)>

---- 'Tackling Deepfakes in European Policy' (2021) PE 690.039

<[https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU\(2021\)690039_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf)>

---- Hahnkamper-Vandenbulcke N and Bacian I, 'Violence against women and domestic violence - The new European Commission proposal in light of European Parliament requests' (2022) PE730.329

<[https://www.europarl.europa.eu/RegData/etudes/STUD/2022/730329/EPRS_STU\(2022\)730329_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/730329/EPRS_STU(2022)730329_EN.pdf)>

Flynn A and others, 'Deepfakes and Digitally Altered Imagery Abuse: A Cross-Country Exploration of an Emerging form of Image-Based Sexual Abuse' (2022) 62 *The British Journal of Criminology* 1341

Franklin S, *The Cambridge Handbook of Artificial Intelligence* (Cambridge University Press, Keith Frankish and William Ramsey 2014)

Franks MA, 'Drafting an Effective "Revenge Porn" Law: A Guide for Legislators' (2015)

<<https://ssrn.com/abstract=2468823>>

Gieseke AP, "'The New Weapon of Choice": Law's Current Inability to Properly Address Deepfake Pornography' (2020) 73 *Vanderbilt Law Review* 1479

Goujard C, 'EU countries reject making non-consensual sex a criminal offense across the bloc' (*Politico*, 9 June 2023) <<https://www.politico.eu/article/rape-europe-criminal-offense-non-consensual-sex/>>

Grady P, 'EU Proposals Will Fail to Curb Nonconsensual Deepfake Porn' (*Center for Data Innovation*, 23 January 2023) <<https://datainnovation.org/2023/01/eu-proposals-will-fail-to-curb-nonconsensual-deepfake-porn/>>

Harris D, 'Deepfakes: False Pornography Is Here and the Law Cannot Protect You' (2019) 17 *Duke Law & Technology Review* 99

HateAid, 'Boundless Hate on the Internet—Dramatic Situation across Europe' (2021)

<https://hateaid.org/wp-content/uploads/2022/04/HateAid-Report-2021_EN.pdf>

Henry N

---- and Powell A, 'Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research' (2018) 19 *Trauma, Violence, & Abuse* 195

---- and Flynn A, 'Image-Based Sexual Abuse: Online Distribution Channels and Illicit Communities of Support' (2019) 25 *Violence Against Women*, 1932

High-Level Expert Group on Artificial Intelligence, 'A Definition of AI: Main Capabilities and Disciplines' (2019)

<https://ec.europa.eu/futurium/en/system/files/ged/ai_hleg_definition_of_ai_18_december_1.pdf>

Karasavva V and Noorbhai A, 'The Real Threat of Deepfake Pornography: A Review of Canadian Policy' (2021) 24 *Cyberpsychology, Behavior, and Social Networking* 203

- Kettunen M, *Legitimizing European Criminal Law* (Springer 2020)
- Kirchengast T, 'Deepfakes and Image Manipulation: Criminalisation and Control' (2020) 29 *Information & Communications Technology Law* 308
- Koops BJ, 'The Internet and its Opportunities for Cybercrime' (2010) Tilburg Law School Legal Studies Research Paper Series No. 09/201
- Klip A, *European criminal law: an integrative approach* (Intersentia 2021)
- Lantwin T, 'Deep Fakes – Düstere Zeiten Für Den Persönlichkeitsschutz? Rechtliche Herausforderungen Und Lösungsansätze' (2019) *MultiMedia Und Recht* <<https://beck-online.beck.de/Dokument?vpath=bibdata%2Fzeits%2FMMR%2F2019%2Fcont%2FMMR.2019.574.1.htm>>
- Mania K, 'Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings From a Comparative Legal Study' (2022) 0 *Trauma, Violence, & Abuse* 1
- Martorana M and Sichi Z, 'Deepfake e revenge porn: punti di contatto' (2021) <<https://www.altalex.com/documents/news/2021/06/03/deepfake-e-revenge-porn-punti-di-contatto>>
- McDermott S and Davies J, 'Deepfaked: 'They put my face on a porn video' (BBC, 21 October 2022) <<https://www.bbc.com/news/uk-62821117>>
- McGlynn C and Rackley E, 'Image-Based Sexual Abuse' (2017) 37 *Oxford Journal of Legal Studies* 534
- Meaker M, 'Europe Has Traded Away Its Online Porn Law' (*Wired UK*, 27 April 2022) <<https://www.wired.co.uk/article/digital-services-act-deepfake-porn>>
- Meskys E and others, 'Regulating Deep Fakes: Legal and Ethical Considerations' (2020) 15 *Journal of Intellectual Property Law & Practice* 24
- Mitsilegas V, *EU Criminal Law* (Hart Publishing 2022)
- O'Halloran A, 'The Technical, Legal, and Ethical Landscape of Deepfake Pornography' (BAThesis, Brown Computer Science 2021)
- Öhman C, 'Introducing the pervert's dilemma: a contribution to the critique of Deepfake Pornography' (2020) 22 *Ethics and Information Technology* 133
- Organisation for Economic Co-operation and Development (OECD), *Recommendation of the Council on Artificial Intelligence*, OECD/LEGAL/0449 (2023)
- Peers S, 'Substantive Criminal Law' in Steve Peers (ed), *EU Justice and Home Affairs Law: Volume II: EU Criminal Law, Policing, and Civil Law* (Oxford 2023)
- Plaha M and Lee J, 'Sharing pornographic deepfakes to be illegal in England and Wales' *BBC* (25 November 2022) <<https://www.bbc.com/news/technology-63669711>>
- Popova M, 'Reading out of context: pornographic deepfakes, celebrity and intimacy' (2020) 7 *Porn Studies* 367
- Rigotti C and McGlynn C, 'Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission's proposal to criminalise image-based sexual abuse' (2022) 13 *New Journal of European Criminal Law* 452

- Rizzica A, 'Sexually explicit deepfakes: to what extent do legal responses protect the depicted persons? - Analysis of the Italian scenario through criminal law, data protection law and right to image' (Master thesis, Tilburg Law School 2021)
- Rodrigues AM, 'Fundamental Rights and Punishment: Is There an EU Perspective' (2019) 10 New J Eur Crim L 17
- Ryan D, 'European remedial coherence in the regulation of non-consensual disclosures of sexual images' (2018) 34 Computer Law Security Review 1053
- Satzger H, *International and European criminal law* (Hart/Nomos 2018)
- 'The Harmonisation of Criminal Sanctions in the European Union - A New Approach' (2019) 2 Eucrim 115
- Schein A, 'When Sharing is Not Caring: Creating an Effective Criminal Framework Free from Specific Intent Provisions to Better Achieve Justice for Victims of Revenge Pornography' (2019) 40 Cardozo Law review 1953
- Scorza G, 'L’Fbi lancia l’allarme: porno-criminali in azione' (*HuffPost*, 12 June 2023).
<https://www.huffingtonpost.it/rubriche/governare-il-futuro/2023/06/12/news/lfb_lancia_lallarme_porno-criminali_in_azione-12361450/>
- Šepece M and Lango M, 'Virtual Revenge Pornography as a New Online Threat to Sexual Integrity' (2020) 15 Balkan Social Science Review 117
- Skórzewska-Amberg M, 'Pornography in Cyberspace - European Regulations' (2011) 5 Masaryk University Journal of Law and Technology 261
- Solowey R, 'A Question of Equivalence: Expanding the Definition of Child Pornography to Encompass “Virtual” Computer-Generated Images' (2002) 4 Tulane Journal of Technology & Intellectual Property 161
- Steinberg S, 'Changing Faces: Morphed Child Pornography Images and the First Amendment' (2019) 68 Emory Law Journal 909
- Stevens D, 'Regulating Deepfake Technology - Legislative possibilities in the Netherlands to obstruct the use of deepfake technology for the creation of non-consensual pornography' (Master thesis, Tilburg Law School 2020)
- Story D and Jenkins R, 'Deepfake Pornography and the Ethics of Non-Veridical Representations' (2023) 36 Philosophy & Technology
- Suslavich B, 'Nonconsensual Deepfakes: A “Deep Problem” for Victims' (2022) Albany Law Journal of Science and Technology, forthcoming <<https://papers.ssrn.com/abstract=4137782>>
- Toparlak RT, 'Criminalising Deep Fake Pornography - A Gender-Specific Analysis of Image-Based Sexual Abuse' (2023) 1 Cognito – studentisches Forum für Recht und Gesellschaft 1
- van der Sloot B, Wagenveld Y and Koops BJ, 'Deepfakes: The Legal Challenges of a Synthetic Society' (2021) Tilburg Institute for Law, Technology, and Society
<<https://www.tilburguniversity.edu/sites/default/files/download/Deepfake%20EN.pdf>>
- Woods L and McGlynn C, 'Pornography platforms, the EU Digital Services Act and Image-Based Sexual Abuse' (*Media@LSE blog*, 26 January 2022)
<<https://blogs.lse.ac.uk/medialse/2022/01/26/pornography-platforms-the-eu-digital-services-act-and-image-based-sexual-abuse/>>

Zeniou NZ, 'Criminal Law Responses to "Revenge Porn" in Cyprus and England: Identification of the Offence and the Need for Legislative Regulations and Prevention' in Tatiana-Eleni Synodinou, Philippe Jogleux, Christiana Markou, Thalia Prastitou-Merdi (eds), *EU Internet Law in the Digital Single Market* (Springer 2021)

ANNEX: LIST OF NATIONAL LAWS AND THEIR TRANSLATION

The following is a list of the national legislations considered during Chapter 3.3 of this research, together with their translation. Countries are presented in alphabetical order.

• BELGIUM

Article 417/9, Code Penal²⁷⁷ - <i>La diffusion non consentie de contenus à caractère sexuel</i> La diffusion non consentie de contenus à caractère sexuel consiste à montrer, rendre accessible ou diffuser du contenu visuel ou audio d'une personne dénudée ou d'une personne qui se livre à une activité sexuelle explicite sans son accord ou à son insu, même si cette personne a consenti à leur réalisation. Cette infraction est punie d'un emprisonnement de six mois à cinq ans. La diffusion non consentie de contenus à caractère sexuel existe dès qu'il y a commencement d'exécution.	Art. 417/9, Belgian Criminal Code²⁷⁸ - <i>Non-consensual sharing of sexual content</i> The non-consensual dissemination of sexual content consists in showing, making accessible or disseminating visual or audio content of a nude person or of a person engaging in explicit sexual activity without their consent or knowledge, even if they have consented to their production. This offence is punishable by imprisonment from six months to five years. The non-consensual dissemination of sexual content is realised as soon as it begins to take place.
--	---

• CROATIA

Članak 144.a, Kazneni zakon²⁷⁹ - <i>Zlouporaba snimke spolno eksplicitnog sadržaja</i> (1) Tko zlouporabi odnos povjerenja i bez pristanka snimane osobe učini dostupnim trećoj osobi snimku spolno eksplicitnog sadržaja koja je snimljena uz pristanak te osobe za osobnu uporabu i na taj način povrijedi privatnost te osobe, kaznit će se kaznom zatvora do jedne godine. (2) Kaznom iz Stavka 1. ovoga članka kaznit će se tko uporabom računalnog sustava ili na drugi način izradi novu ili preinači postojeću snimku spolno eksplicitnog	Article 144a, Croatian Criminal Code²⁸⁰ - <i>Misuse of recordings of sexually explicit content</i> (1) Whoever violates trust and without consent from the recorded person makes the recording of sexually explicit content, which was filmed with consent from the recorded person for personal use, available to a third party, thus violating the privacy of the recorded person, will be sentenced to up to 1 year of jail time. (2) Whoever creates a new recording of sexually explicit content or modifies the existing one, by use of a computer system or in any other way, and uses it as the authentic one, thus violating the privacy of the person in
---	--

²⁷⁷ Official text available at

<https://www.ejustice.just.fgov.be/cgi_loi/loi_a1.pl?DETAIL=1867060801%2FF&caller=list&row_id=1&numero=2&rech=4&cn=1867060801&table_name=LOI&nm=1867060850&la=F&dt=CODE+PENAL&language=fr&fr=f&choix1=ET&choix2=ET&fromtab=loi_all&trier=promulgation&chercher=t&sql=dt+contains++%27CODE%27%26+%27PENAL%27and+actif+%3D+%27Y%27&tri=dd+AS+RANK+&imgcn.x=41&imgcn.y=12#LNK0114> accessed 27 April 2024.

²⁷⁸ Own translation.

²⁷⁹ Unofficial text available at <<https://www.zakon.hr/z/98/Kazneni-zakon>> accessed 27 April 2024.

²⁸⁰ Text translated with the online free translator “DeepL” <<https://www.deepl.com/translator>>.

sadržaja I tu snimku uporabi kao pravu te time provrijedi privatnost osobe na toj snimci.	the recording, will be sentenced in accordance to the penalty from paragraph 1. of this article.
(3) Tko kazneno djelo iz stavka 1. i 2. ovoga članka počini putem računalnog sustava ili mreže ili na drugi način zbog čega je snimka postala dostupna većem broju osoba, kaznit će se kaznom zatvora do tri godine.	(3) Whoever commits an offence from paragraphs 1. and 2. of this article by use of a computer system, network or in any other way that allows the recording to become available to more people, will be sentenced to up to 3 years of jail time.
(4) Kazneno djelo iz stavka 1., 2. i 3. ovoga članka progoni se po prijedlogu.	(4) Felonies from paragraphs 1., 2. and 3. of this article are prosecuted according to this proposal.
(5) Snimke i posebne naprave kojima je počinjeno kazneno djelo iz ovoga članka će se oduzeti.	(5) The recordings and devices used to commit the felony will be confiscated.

• FRANCE

Article 226-1, Code pénal ²⁸¹	Article 226-1, French Criminal Code ²⁸²
Est puni d'un an d'emprisonnement et de 45 000 euros d'amende le fait, au moyen d'un procédé quelconque, volontairement de porter atteinte à l'intimité de la vie privée d'autrui:	It is punishable by one year's imprisonment and a fine of 45,000 euros to wilfully violate the privacy of another person by any means whatsoever:
1° En captant, enregistrant ou transmettant, sans le consentement de leur auteur, des paroles prononcées à titre privé ou confidentiel;	1° By capturing, recording or transmitting, without the author's consent, words spoken in private or in confidence;
2° En fixant, enregistrant ou transmettant, sans le consentement de celle-ci, l'image d'une personne se trouvant dans un lieu privé.	2° By capturing, recording or transmitting, without the consent of the person concerned, the image of a person in a private place.
3° En captant, enregistrant ou transmettant, par quelque moyen que ce soit, la localisation en temps réel ou en différé d'une personne sans le consentement de celle-ci.	3° By capturing, recording or transmitting, by any means whatsoever, the real-time or deferred location of a person without that person's consent.
Lorsque les actes mentionnés aux 1° et 2° du présent article ont été accomplis au vu et au su des intéressés sans qu'ils s'y soient opposés, alors qu'ils étaient en mesure de le faire, le consentement de ceux-ci est présumé.	When the acts mentioned in 1° and 2° of the present article have been carried out in full view of the interested parties without their having objected, even though they were in a position to do so, their consent is presumed.
Lorsque les actes mentionnés au présent article ont été accomplis sur la personne d'un mineur, le consentement doit émaner des titulaires de l'autorité parentale, dans le respect de l'article 372-1 du code civil.	Where the acts referred to in this article have been performed on a minor, consent must be given by the holders of parental authority, in compliance with article 372-1 of the French Civil Code.
Lorsque les faits sont commis par le conjoint ou le concubin de la victime ou le partenaire lié à la victime par un pacte civil de solidarité, les peines sont portées	When the acts are committed by the victim's spouse or cohabitee, or by a partner bound to the victim by a civil solidarity pact, the penalties are increased to two years' imprisonment and a fine of 60,000 euros.

²⁸¹ Official text available at

<https://www.legifrance.gouv.fr/codes/section_lc/LEGITEXT000006070719/LEGISCTA000006165309/#LEGISCTA000006165309> accessed 27 April 2024.

²⁸² Own translation.

à deux ans d'emprisonnement et à 60 000 euros d'amende.	
Article 226-2, Code pénal Est puni des mêmes peines le fait de conserver, porter ou laisser porter à la connaissance du public ou d'un tiers ou d'utiliser de quelque manière que ce soit tout enregistrement ou document obtenu à l'aide de l'un des actes prévus par l'article 226-1. Lorsque le délit prévu par l'alinéa précédent est commis par la voie de la presse écrite ou audiovisuelle, les dispositions particulières des lois qui régissent ces matières sont applicables en ce qui concerne la détermination des personnes responsables.	Article 226-2, French Criminal Code The same penalties apply to keeping, bringing or allowing to be brought to the attention of the public or a third party, or using in any way whatsoever any recording or document obtained by means of one of the acts provided for in article 226-1. Where the offence referred to in the previous paragraph is committed via the written or audiovisual press, the specific provisions of the laws governing these subjects shall apply to the determination of the persons liable.
Article 226-2-1, Code pénal Lorsque les délits prévus aux articles 226-1 et 226-2 portent sur des paroles ou des images présentant un caractère sexuel prises dans un lieu public ou privé, les peines sont portées à deux ans d'emprisonnement et à 60 000 € d'amende. Est puni des mêmes peines le fait, en l'absence d'accord de la personne pour la diffusion, de porter à la connaissance du public ou d'un tiers tout enregistrement ou tout document portant sur des paroles ou des images présentant un caractère sexuel, obtenu, avec le consentement exprès ou présumé de la personne ou par elle-même, à l'aide de l'un des actes prévus à l'article 226-1.	Article 226-2-1, French Criminal Code When the offences provided for in articles 226-1 and 226-2 concern words or images of a sexual nature taken in a public or private place, the penalties are increased to two years' imprisonment and a €60,000 fine. The same penalties apply to the fact of making known to the public or to a third party, without the person's consent to broadcast, any recording or document of words or images of a sexual nature, obtained, with the express or implicit consent of the person or by the person him/herself, by means of one of the acts provided for in article 226-1.

• GERMANY

§201a, Strafgesetzbuch (StGB)²⁸³ - <i>Verletzung des höchstpersönlichen Lebensbereichs und von Persönlichkeitsrechten durch Bildaufnahmen</i> (1) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer 1. von einer anderen Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, unbefugt eine Bildaufnahme herstellt oder überträgt und dadurch den höchstpersönlichen Lebensbereich der abgebildeten Person verletzt, 2. eine Bildaufnahme, die die Hilflosigkeit einer anderen Person zur Schau stellt, unbefugt herstellt oder überträgt und dadurch den höchstpersönlichen Lebensbereich der abgebildeten Person verletzt,	Section 201a, German Criminal Code²⁸⁴ - <i>Violation of intimate privacy and of rights of personality by taking photographs or other images</i> (1) Whoever 1. without being authorised to do so creates or transmits photographs or other images of another person in private premises or in a room which is specially protected from view, and thereby violates the intimate privacy of the person depicted, 2. without being authorised to do so produces a photograph or other image exhibiting the helplessness of another person or transmits such image, and thereby violates the intimate privacy of the person depicted, 3. without being authorised to do so creates or transmits a photograph or other image which in
--	---

²⁸³ Official text available at <https://www.gesetze-im-internet.de/stgb/_201a.html> accessed 27 April 2024

²⁸⁴ Official translation available at <https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html> accessed 27 April 2024.

3. eine Bildaufnahme, die in grob anstößiger Weise eine verstorbene Person zur Schau stellt, unbefugt herstellt oder überträgt, 4. eine durch eine Tat nach den Nummern 1 bis 3 hergestellte Bildaufnahme gebraucht oder einer dritten Person zugänglich macht oder 5. eine befugt hergestellte Bildaufnahme der in den Nummern 1 bis 3 bezeichneten Art wissentlich unbefugt einer dritten Person zugänglich macht und in den Fällen der Nummern 1 und 2 dadurch den höchstpersönlichen Lebensbereich der abgebildeten Person verletzt. (2) Ebenso wird bestraft, wer unbefugt von einer anderen Person eine Bildaufnahme, die geeignet ist, dem Ansehen der abgebildeten Person erheblich zu schaden, einer dritten Person zugänglich macht. Dies gilt unter den gleichen Voraussetzungen auch für eine Bildaufnahme von einer verstorbenen Person. (3) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe wird bestraft, wer eine Bildaufnahme, die die Nacktheit einer anderen Person unter achtzehn Jahren zum Gegenstand hat, 1. herstellt oder anbietet, um sie einer dritten Person gegen Entgelt zu verschaffen, oder 2. sich oder einer dritten Person gegen Entgelt verschafft. (4) Absatz 1 Nummer 2 und 3, auch in Verbindung mit Absatz 1 Nummer 4 oder 5, Absatz 2 und 3 gelten nicht für Handlungen, die in Wahrnehmung überwiegender berechtigter Interessen erfolgen, namentlich der Kunst oder der Wissenschaft, der Forschung oder der Lehre, der Berichterstattung über Vorgänge des Zeitgeschehens oder der Geschichte oder ähnlichen Zwecken dienen. (5) Die Bildträger sowie Bildaufnahmegeräte oder andere technische Mittel, die der Täter oder Teilnehmer verwendet hat, können eingezogen werden. § 74a ist anzuwenden.	a grossly offensive manner exhibits a deceased person, 4. uses a photograph or other image produced by an offence under no. 1 to no. 3 or makes it available to a third party or 5. makes available to a third party, in the awareness of lacking authorisation to do so, a photograph or other image of the type set out in no. 1 to no. 3 which was produced with authorisation, and, in the cases under no. 1 and no. 2, thereby violates the intimate privacy of the person depicted, incurs a penalty of imprisonment for a term not exceeding two years or a fine. (2) Whoever, without being authorised to do so, makes available to a third party a photograph or other image of another person which is of such a nature as to significantly damage the reputation of the person depicted incurs the same penalty. This also applies, under the same conditions, to a photograph or other image of a deceased person. (3) Whoever 1. produces or offers to procure for a third party for a consideration or 2. procures for themselves or for a third party for a consideration an image showing the nakedness of another person under 18 years of age incurs a penalty of imprisonment for a term not exceeding two years or a fine. (4) Subsection (1) no. 2 and no. 3, also in conjunction with subsection (1) no. 4 or no. 5, and subsections (2) and (3) do not apply to activities done by way of exercising overriding legitimate interests, namely those serving the arts or science, research or teaching, to report about current or historical events, or for similar purposes. (5) The image media and image recording devices or other technical means used by the offender or participant may be confiscated. Section 74a applies.
---	---

• IRELAND

Article 2, Harassment, Harmful Communications and Related Offences Act 2020, Number 32 of 2020²⁸⁵ - <i>Distributing, publishing or threatening to distribute or publish intimate image without consent with intent to cause harm or being reckless as to whether harm is caused</i>	
---	--

²⁸⁵ Official text available at <<https://www.irishstatutebook.ie/eli/2020/act/32/enacted/en/pdf>> accessed 27 April 2024.

(1) A person who distributes, publishes or threatens to distribute or publish an intimate image of another person— (a) without that other person's consent, and (b) with intent to cause harm to, or being reckless as to whether or not harm is caused to, the other person, is guilty of an offence. (2) For the purposes of subsection (1), a person causes harm to another person where— (a) he or she, by his or her acts, intentionally or recklessly seriously interferes with the other person's peace and privacy or causes alarm or distress to the other person, and (b) his or her acts are such that a reasonable person would realise that the acts would seriously interfere with the other person's peace and privacy or cause alarm or distress to the other person. (3) A person who is guilty of an offence under this section is liable— (a) on summary conviction to a class A fine or imprisonment for a term not exceeding 12 months, or both, or (b) on conviction on indictment to a fine or imprisonment for a term not exceeding seven years, or both.	
---	--

• **ITALY**

Articolo 612-ter, Codice Penale²⁸⁶ - <i>Diffusione illecita di immagini o video sessualmente espliciti</i> 1. Salvo che il fatto costituisca più grave reato, chiunque, dopo averli realizzati o sottratti, invia, consegna, cede, pubblica o diffonde immagini o video a contenuto sessualmente esplicito, destinati a rimanere privati, senza il consenso delle persone rappresentate, è punito con la reclusione da uno a sei anni e con la multa da euro 5.000 a euro 15.000. 2. La stessa pena si applica a chi, avendo ricevuto o comunque acquisito le immagini o i video di cui al primo comma, li invia, consegna, cede, pubblica o diffonde senza il consenso delle persone rappresentate al fine di recare loro nocumento. 3. La pena è aumentata se i fatti sono commessi dal coniuge, anche separato o divorziato, o da persona che è o è stata legata da relazione affettiva alla persona offesa ovvero se i fatti sono commessi attraverso strumenti informatici o telematici.	Article 612-ter, Italian Criminal Code²⁸⁷ - <i>Unlawful dissemination of sexually explicit images or videos</i> 1. Unless the act constitutes a more serious crime, anyone who, after having made or taken them, sends, delivers, assigns, publishes or disseminates images or videos with sexually explicit content, intended to remain private, without the consent of the persons depicted, shall be punished by imprisonment from one to six years and a fine from 5,000 to 15,000 euros. 2. The same punishment shall apply to any person who, having received or otherwise acquired the images or videos referred to in the first paragraph, sends, delivers, assigns, publishes or disseminates them without the consent of the persons represented for the purpose of causing them harm. 3. The punishment shall be increased if the acts are committed by the spouse, including a separated or divorced spouse, or by a person who is or has been in a sentimental relationship with the offended person or if
--	--

²⁸⁶ Official text available at <<https://legislation.mt/eli/cap/9/eng/pdf>> accessed 27 April 2024.

²⁸⁷ Own translation.

4. La pena è aumentata da un terzo alla metà se i fatti sono commessi in danno di persona in condizione di inferiorità fisica o psichica o in danno di una donna in stato di gravidanza. 5. Il delitto è punito a querela della persona offesa. Il termine per la proposizione della querela è di sei mesi. La remissione della querela può essere soltanto processuale. Si procede tuttavia d'ufficio nei casi di cui al quarto comma, nonché quando il fatto è connesso con altro delitto per il quale si deve procedere d'ufficio.	the acts are committed through computer or telematic means. 4. The punishment is increased by one-third to one-half if the acts are committed against a person in a condition of physical or mental inferiority or against a pregnant woman. 5. The crime is punishable on complaint by the offended person. The time limit for filing a complaint shall be six months. The dismissal of the complaint may only be procedural. However, it shall be prosecuted ex officio in the cases referred to in paragraph four, as well as when the fact is related to another crime that must be prosecuted ex officio.
---	---

• MALTA

Article 208E, Maltese Criminal Code²⁸⁸ - <i>Non-consensual taking or disclosure of private sexual photographs and films</i> (1) Whosoever, with an intent to cause distress, emotional harm or harm of any nature, takes or discloses a private sexual photograph or film without the consent of the person or persons displayed or depicted in such photograph or film shall on conviction be liable to imprisonment for a term of up to five years or to a fine (<i>multa</i>) of not less than four thousand euro (€4,000) and not more than eight thousand euro (€8,000), or to both such imprisonment and fine.	
---	--

• PORTUGAL

Artigo 192, Código Penal²⁸⁹ - <i>Devassa da vida privada</i> 1 - Quem, sem consentimento e com intenção de devassar a vida privada das pessoas, designadamente a intimidade da vida familiar ou sexual: a) Interceptar, gravar, registar, utilizar, transmitir ou divulgar conversa, comunicação telefónica, mensagens de correio electrónico ou facturação detalhada; b) Captar, fotografar, filmar, registar ou divulgar imagem das pessoas ou de objectos ou espaços íntimos; c) Observar ou escutar às ocultas pessoas que se encontrem em lugar privado; ou d) Divulgar factos relativos à vida privada ou a doença grave de outra pessoa; é punido, no caso das alíneas a) e c), com pena de prisão até 1 ano ou pena de multa até 240 dias e, no caso das	Article 192, Portuguese Criminal Code²⁹⁰ - <i>Breach of privacy</i> 1 - Whoever, without consent and with the intention of invading the private life of a person, namely the intimacy of family or sexual life: a) Intercepts, records, uses, transmits or discloses conversations, telephone communications, e-mail messages or detailed invoices; b) Captures, photographs, films, records or disseminates images of people or intimate objects or spaces; c) Observes or eavesdrops on persons in a private place; or d) Discloses facts about another person's private life or serious illness; shall be punishable, in the case of subparagraphs a) and c), by imprisonment for a term not exceeding one year or a fine not exceeding 240 days and, in the case of
--	---

²⁸⁸ Official text available at <<https://legislation.mt/eli/cap/9/eng/pdf>> accessed 27 April 2024.

²⁸⁹ Official text available at <<https://diariodarepublica.pt/dr/legislacao-consolidada/decreto-lei/1995-34437675>> accessed 27 April 2024.

²⁹⁰ Text translated with the online free translator “DeepL” <<https://www.deepl.com/translator>>.

alíneas b) e d), com pena de prisão até 3 anos ou com pena de multa.	subparagraphs b) and d), by imprisonment for a term not exceeding three years or a fine.
2 - O facto previsto na alínea d) do número anterior não é punível quando for praticado como meio adequado para realizar um interesse público legítimo e relevante.	2 - The act provided for in point d) of the previous paragraph shall not be punishable if it is carried out as an appropriate means to achieve a legitimate and relevant public interest.

• ROMANIA

Articolul 4(1)(h), Legea nr. 217 din 22 mai 2003 pentru prevenirea și combaterea violenței domestice ²⁹¹	Article 4(1)(h), Law no. 217 of 22 May 2003 to prevent and combat domestic violence ²⁹²
(1) Violența domestică se manifestă sub următoarele forme: [...] (h) violența cibernetică - hărțuire online, mesaje online instigatoare la ură pe bază de gen, urmărire online, amenințări online, publicarea nonconsensuală de informații și conținut grafic intim, accesul ilegal de interceptare a comunicațiilor și datelor private și orice altă formă de utilizare abuzivă a tehnologiei informației și a comunicațiilor prin intermediul calculatoarelor, telefoanelor mobile inteligente sau altor dispozitive similare care folosesc telecomunicațiile sau se pot conecta la internet și pot transmite și utiliza platformele sociale sau de e-mail, cu scopul de a face de rușine, umili, speria, amenința, reduce la tăcere victima.	(1) Domestic violence manifests itself in the following forms: [...] (h) cyber violence - online harassment, online messages inciting gender-based hatred, online stalking, online threats, non-consensual publication of intimate information and graphic content, unlawful access to intercept private communications and data, and any other form of misuse of information and communication technology through computers, smart mobile phones or other similar devices that use telecommunications or can connect to the internet and transmit and use social or email platforms, with the purpose of shaming, humiliating, frightening, threatening, silencing the victim.

• SLOVAK REPUBLIC

§360b Nebezpečné elektronické obťažovanie, Trestný zákon ²⁹³	§360b Dangerous electronic harassment, Slovakian Criminal Code ²⁹⁴
(1) Kto úmyselne prostredníctvom elektronickej komunikačnej služby, počítačového systému alebo počítačovej siete podstatným spôsobom zhorší kvalitu života iného tým, že a) ho dlhodobo ponízuje, zastrašuje, neoprávnene koná v jeho mene alebo dlhodobo inak obťažuje, alebo b) neoprávnene zverejní alebo sprístupní tretej osobe obrazový, zvukový alebo obrazovo-zvukový záznam jeho prejavu osobnej povahy získaný s jeho súhlasom, spôsobilý značnou mierou ohroziť jeho vážnosť alebo privodiť mu inú vážnu ujmu na právach, potrestá sa odňatím slobody až na tri roky. (2) Odňatím slobody na jeden rok až štyri roky sa páchatel potrestá, ak spácha čin uvedený v odseku 1 a) na chránenej osobe, alebo	(1) Whoever intentionally, by means of an electronic communication service, computer system or computer network, substantially impairs the quality of life of another by (a) humiliating, intimidating, wrongfully acting on behalf of or otherwise harassing him or her for a prolonged period of time; or (b) unlawfully disclosing or making available to a third party a visual, audio or visual-audio recording of his or her speech of a personal nature, obtained with his or her consent, which is capable of materially impairing his or her reputation or otherwise causing him or her serious injury to his or her rights, shall be punishable by imprisonment for a term of up to three years.

²⁹¹ Official text available at <<https://legislatie.just.ro/Public/DetaliuDocument/44014>> accessed 27 April 2024.

²⁹² Text translated with the online free translator “DeepL” <<https://www.deepl.com/translator>>.

²⁹³ Unofficial text available at <https://www.autora.sk/zz/2005/300/#sect360b_Nebezpen_elektronick_obaovanie> accessed 27 April 2024.

²⁹⁴ Text translated with the online free translator “DeepL” <<https://www.deepl.com/translator>>.

b) z osobitného motívu. (3) Odňatím slobody na dva roky až šesť rokov sa páchatel potrestá, ak spácha čin uvedený v odseku 1 a) a spôsobí ním značnú škodu, b) s úmyslom získať pre seba alebo iného značný prospech, alebo c) hoci bol za taký čin v predchádzajúcich dvadsiatich štyroch mesiacoch odsúdený.	(2) The offender shall be sentenced to imprisonment for a term of one to four years if he commits an act referred to in paragraph 1 a) on a protected person, or b) for a special motive. (3) An offender shall be liable to imprisonment for a term of between two and six years if he commits an act referred to in paragraph 1 (a) and causes substantial damage thereby, (b) with intent to obtain for himself or another a substantial benefit, or (c) although he has been convicted of such an offence within the preceding twenty-four months.
---	---

• SLOVENIA

143. člen, Kazenski Zakonik²⁹⁵ - <i>Zloraba osebnih podatkov</i> (1) Kdor brez podlage v zakonu ali v osebni privolitvi posameznika, na katerega se osebni podatki nanašajo, osebne podatke, ki se obdelujejo na podlagi zakona ali osebne privolitve posameznika, posreduje v javno objavo ali jih javno objavi, se kaznuje z denarno kaznijo ali zaporom do enega leta. (2) Enako se kaznuje, kdor vdre ali nepooblaščen vstopi v računalniško vodeno zbirko podatkov z namenom, da bi sebi ali komu drugemu pridobil kakšen osebni podatek. (3) Kdor na svetovnem medmrežju ali drugače javno objavi ali omogoči drugemu objavo osebnih podatkov žrtev kaznivih dejanj, žrtev kršitev pravic ali svoboščin, zaščiteneh prič, ki se nahajajo v sodnih spisih sodnih postopkov, kjer po zakonu ali po odločitvi sodišča ni dovoljena prisotnost javnosti ali identifikacija žrtev ali zaščiteneh prič ter osebnih zapisov o njih v zvezi s sodnim postopkom, na podlagi katerih se te osebe lahko določi ali so določljive, se kaznuje z zaporom do treh let. (4) Kdor prevzame identiteto druge osebe ali z obdelavo njenih osebnih podatkov izkorišča njene pravice, si na njen račun pridobiva premoženjsko ali nepremoženjsko korist ali prizadene njeno osebno dostojanstvo, se kaznuje z zaporom od treh mesecev do treh let.	Article 143 Slovenian Criminal Code²⁹⁶ - <i>Abuse of personal data</i> (1) Whoever publishes or causes to be published personal data processed on the basis of the law or the personal consent of the individual to whom the personal data relate without any basis in law or without the personal consent of the individual shall be punished by a fine or sentenced to up to one year in prison. (2) Whoever breaks into a computer database in order to acquire personal data for his or a third person's use shall be punished in accordance with the preceding paragraph. (3) Whoever publishes on the internet or otherwise publishes or enables another person to publish personal data of victims of criminal offences, victims of violation of rights and liberties, protected witnesses, which are contained in judicial records of court proceedings, in which the presence of the public or witness identification or protected witnesses and personal records thereof related to the court proceeding was not allowed according to the law or court decision, on the basis of which these persons may be identified or are identifiable, shall be sentenced to imprisonment for not more than three years. (4) Whoever assumes the identity of another person or, by processing his or her personal data, exploits his or her rights, gains proceeds or non-pecuniary benefits or adversely affects his or her personal dignity shall be sentenced to between three months and three years in prison.
--	--

²⁹⁵ Unofficial text available at

<https://www.unodc.org/uploads/icsant/documents/Legislation/Slovenia/Criminal_Code_-_Slovenia.pdf> accessed 27 April 2024.

²⁹⁶ Unofficial translational available at

<https://www.unodc.org/uploads/icsant/documents/Legislation/Slovenia/Criminal_Code_-_Slovenia.pdf> accessed 27 April 2024.

(5) Kdor stori dejanje iz prvega odstavka tega člena tako, da posreduje v javno objavo ali javno objavi občutljive osebne podatke, se kaznuje z zaporom do dveh let. (6) Kdor javno objavi posnetke ali sporočila druge osebe s seksualno vsebino brez privolitve te osebe in s tem huje prizadene njeno zasebnost, se kaznuje z zaporom od treh mesecev do treh let. (7) Če stori dejanje iz prejšnjih odstavkov tega člena uradna oseba z zlorabo uradnega položaja ali uradnih pravic, se kaznuje z zaporom do petih let. (8) Pregon iz četrtega in šestega odstavka tega člena se začne na predlog.	(5) Whoever commits the offence referred to in paragraph one of this Article by publishing or causing to be published sensitive personal data shall be sentenced to up to two years in prison. (6) Whoever publishes photographs or videos with sexual content of another person without that person's consent and thereby severely affects that person's privacy, shall be sentenced to imprisonment from three months to three years. (7) If any offence referred to in the preceding paragraphs of this Article is committed by an official through the abuse of office or official authority, such an official shall be sentenced to imprisonment for not more than five years. (8) The prosecution referred to in paragraphs four and six of this Article shall be initiated upon a complaint.
---	---

• **SPAIN**

Artículo 197, Código Penal.²⁹⁷ 1. El que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas, mensajes de correo electrónico o cualesquiera otros documentos o efectos personales, intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses. 2. Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero. 3. Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores. Será castigado con las penas de prisión de uno a tres años y multa de doce a veinticuatro meses, el que, con conocimiento de su origen ilícito y sin haber tomado parte en su descubrimiento, realizare la conducta descrita en el párrafo anterior.	Article 197, Spanish Criminal Code²⁹⁸ 1. Whoever, in order to discover the secrets or violate the privacy of another, without his consent, seizes his papers, letters, electronic mail messages or any other documents or personal effects, intercepts his telecommunications or uses technical devices for listening, transmission, recording or reproduction of sound or image, or of any other communication signal, shall be punished with imprisonment of one to four years and a fine of twelve to twenty-four months. 2. The same penalties shall be imposed on anyone who, without being authorized, seizes, uses or modifies, to the detriment of a third party, reserved data of a personal or family nature of another person that is recorded in computer, electronic or telematic files or media, or in any other type of public or private file or record. The same penalties shall be imposed on anyone who, without being authorized, accesses them by any means, and on anyone who alters or uses them to the detriment of the owner of the data or of a third party. 3. A prison sentence of two to five years shall be imposed if the data or facts discovered or the images captured referred to in the preceding paragraphs are disseminated, disclosed or transferred to third parties. A term of imprisonment of one to three years and a fine of twelve to twenty-four months shall be imposed on anyone who, with knowledge of its unlawful origin and without having taken part in its discovery, engages in the conduct described in the preceding paragraph.
--	---

²⁹⁷ Official text available at <<https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444>> accessed 27 April 2024.

²⁹⁸ Text translated with the online free translator “DeepL” <<https://www.deepl.com/translator>>.

4. Los hechos descritos en los apartados 1 y 2 de este artículo serán castigados con una pena de prisión de tres a cinco años cuando: a) Se cometan por las personas encargadas o responsables de los ficheros, soportes informáticos, electrónicos o telemáticos, archivos o registros; o b) se lleven a cabo mediante la utilización no autorizada de datos personales de la víctima. Si los datos reservados se hubieran difundido, cedido o revelado a terceros, se impondrán las penas en su mitad superior. 5. Igualmente, cuando los hechos descritos en los apartados anteriores afecten a datos de carácter personal que revelen la ideología, religión, creencias, salud, origen racial o vida sexual, o la víctima fuere un menor de edad o una persona con discapacidad necesitada de especial protección, se impondrán las penas previstas en su mitad superior. 6. Si los hechos se realizan con fines lucrativos, se impondrán las penas respectivamente previstas en los apartados 1 al 4 de este artículo en su mitad superior. Si además afectan a datos de los mencionados en el apartado anterior, la pena a imponer será la de prisión de cuatro a siete años. 7. Será castigado con una pena de prisión de tres meses a un año o multa de seis a doce meses el que, sin autorización de la persona afectada, difunda, revele o ceda a terceros imágenes o grabaciones audiovisuales de aquella que hubiera obtenido con su anuencia en un domicilio o en cualquier otro lugar fuera del alcance de la mirada de terceros, cuando la divulgación menoscabe gravemente la intimidad personal de esa persona. Se impondrá la pena de multa de uno a tres meses a quien habiendo recibido las imágenes o grabaciones audiovisuales a las que se refiere el párrafo anterior las difunda, revele o ceda a terceros sin el consentimiento de la persona afectada. En los supuestos de los párrafos anteriores, la pena se impondrá en su mitad superior cuando los hechos hubieran sido cometidos por el cónyuge o por persona que esté o haya estado unida a él por análoga relación de afectividad, aun sin convivencia, la víctima fuera menor de edad o una persona con discapacidad necesitada de especial protección, o los hechos se hubieran cometido con una finalidad lucrativa.	4. The acts described in paragraphs 1 and 2 of this article shall be punished with a prison sentence of three to five years when: (a) are committed by the persons in charge or responsible for the files, computer, electronic or telematic supports, archives or registers; or. b) are carried out through the unauthorized use of personal data of the victim. If the confidential data had been disseminated, transferred or disclosed to third parties, the penalties shall be imposed in the upper half. 5. Likewise, when the facts described in the preceding paragraphs affect personal data revealing ideology, religion, beliefs, health, racial origin or sex life, or the victim is a minor or a disabled person in need of special protection, the penalties provided for in its upper half shall be imposed. 6. If the acts are carried out for lucrative purposes, the penalties provided for in paragraphs 1 to 4 of this article shall be imposed in their upper half. If they also affect data mentioned in the preceding paragraph, the penalty to be imposed shall be imprisonment for a term of four to seven years. 7. A prison sentence of three months to one year or a fine of six to twelve months shall be imposed on anyone who, without the authorization of the person concerned, disseminates, discloses or transfers to third parties images or audiovisual recordings of that person obtained with his consent in a home or any other place beyond the reach of the gaze of third parties, when the disclosure seriously undermines the personal privacy of that person. A fine of one to three months shall be imposed on anyone who, having received the images or audiovisual recordings referred to in the preceding paragraph, disseminates, discloses or transfers them to third parties without the consent of the person concerned. In the cases of the preceding paragraphs, the penalty will be imposed in its upper half when the facts had been committed by the spouse or by a person who is or has been united to him/her by analogous relationship of affectivity, even without cohabitation, the victim was a minor or a person with disabilities in need of special protection, or the facts had been committed with a lucrative purpose.
---	---

- **SWEDEN**

4 kap., §6a, Brottsbalk (1962:700)²⁹⁹ Den som olovligen med tekniskt hjälpmedel i hemlighet tar upp bild av någon som befinner sig inomhus i en bostad eller på en toalett, i ett omklädningsrum eller ett annat liknande utrymme, döms för kränkande fotografering till böter eller fängelse i högst två år. Till ansvar ska det inte dömas om gärningen med hänsyn till syftet och övriga omständigheter är försvarlig. Första stycket gäller inte den som med tekniskt hjälpmedel tar upp bild av någon som ett led i en myndighets verksamhet.	Chapter 4, Section 6a, Swedish Criminal Code³⁰⁰ Anyone who unlawfully uses technical means to secretly take a picture of someone who is indoors in a dwelling or in a toilet, changing room or other similar space shall be sentenced for intrusive photography to a fine or imprisonment for a maximum of two years. Liability shall not be imposed if the act is justifiable given the purpose and other circumstances. The first paragraph does not apply to anyone who uses technical means to take a picture of someone as part of an authority's activities.
4 kap., §6c, Brottsbalk (1962:700) Den som gör intrång i någon annans privatliv genom att sprida 1. bild på eller annan uppgift om någons sexualliv, 2. bild på eller annan uppgift om någons hälsotillstånd, 3. bild på eller annan uppgift om att någon utsatts för ett brott som innefattar ett angrepp mot person, frihet eller frid, 4. bild på någon som befinner sig i en mycket utsatt situation, eller 5. bild på någons helt eller delvis nakna kropp döms, om spridningen är ägnad att medföra allvarlig skada för den som bilden eller uppgiften rör, för olaga integritetsintrång till böter eller fängelse i högst två år. Det ska inte dömas till ansvar om gärningen med hänsyn till syftet och övriga omständigheter var försvarlig.	Chapter 4, Section 6c, Swedish Criminal Code Anyone who infringes someone else's private life by disseminating 1. a picture or other information about someone's sex life, 2. an image or other information about someone's state of health, 3. an image or other information that someone has been subjected to a crime involving an attack on the person, freedom or peace, 4. an image of someone in a highly vulnerable situation; or 5. an image of someone's fully or partially naked body. is sentenced, if the dissemination is likely to cause serious harm to the person to whom the image or information relates, for unlawful invasion of privacy to a fine or imprisonment for a maximum of two years. Liability shall not be imposed if the act was justifiable in view of the purpose and other circumstances.

• THE NETHERLANDS

Artikel 139h, Wetboek van Strafrecht³⁰¹ 1 Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft: a. hij die opzettelijk en wederrechtelijk van een persoon een afbeelding van seksuele aard vervaardigt; b. hij die de beschikking heeft over een afbeelding als bedoeld onder a terwijl hij weet of redelijkerwijs moet vermoeden dat deze door of als gevolg van een onder a strafbaar gestelde handeling is verkregen.	Article 139h, Dutch Criminal Code³⁰² 1 With imprisonment of up to one year or a fine of the fourth category is punished: a. he who intentionally and unlawfully produces an image of a person of a sexual nature; b. he who has at his disposal an image as referred to under a while he knows or should reasonably suspect that it has been obtained by or as a result of an act punishable under a. 2 May be punished with imprisonment of not more than two years or a fine of the fourth category:
--	---

²⁹⁹ Official text available at <https://www.riksdagen.se/sv/dokument-och-lagar/dokument/svensk-forfattningssamling/brottsbalk-1962700_sfs-1962-700/#K4> accessed 27 April 2024.

³⁰⁰ Text translated with the online free translator "DeepL" <<https://www.deepl.com/translator>>.

³⁰¹ Official text available at <<https://wetten.overheid.nl/BWBR0001854/2024-01-01>> accessed 27 April 2024.

³⁰² Text translated with the online free translator "DeepL" <<https://www.deepl.com/translator>>.

2 Met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie wordt gestraft: a. hij die een afbeelding als bedoeld in het eerste lid, onder a, openbaar maakt terwijl hij weet of redelijkerwijs moet vermoeden dat deze door of als gevolg van een in het eerste lid, onder a, strafbaar gestelde handeling is verkregen; b. hij die van een persoon een afbeelding van seksuele aard openbaar maakt, terwijl hij weet dat die openbaarmaking nadelig voor die persoon kan zijn.	a. he who publishes an image as referred to in the first paragraph under a, while he knows or should reasonably suspect that it has been obtained by or as a result of an act punishable under the first paragraph under a; b. he who discloses an image of a person of a sexual nature while he knows that such disclosure may be detrimental to that person.
---	--