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.

Andrea Rizzica
SNR: 1276491
ANR: 934098

Master's Thesis Law and Technology
Tilburg Law School

Tilburg, 29th April 2021

TFG 4 – Crime and security in the information age
First reader: Lucas Jones
Second reader: Siddharth Peter de Souza

Word count (excluding table of contents, footnotes and bibliography): 17427

Table of contents

Chapter I: Introduction

1.1. Background

The so called deepfake technology is developing rapidly and it is defined as a video, photo, audio recording that seems real but has been manipulated with Artificial Intelligence (AI):[1] "it implies the replacement of the face of person A with the face of person B. In the meantime, person A's facial expressions, movements and environs are duplicated but with the face of person B instead. In short, deepfakes make it possible to swap one person's face in an image or video with the face of another person".[2] The output is a video or image which is intended to realistically represent a chosen subject. Notably, deepfake technology utilizes the artificial intelligence technique known as deep learning[3] to identify and swap faces into photos and videos: it analyzes a large amount of pictures or records with somebody's face, training an AI algorithm to manipulate it and then uses that algorithm to map the face onto another person in another video.[4] Although this technique may have legitimate uses, for example in the field of satirical entertainment,[5] it can also be utilized to commit harm, for example by making it look like a person in a pornographic video she/he was not in fact in and by spreading the video online with the name of the depicted person.[6]

The result of deepfake videos can be extremely accurate[7] and ethical consequences may develop from their publication, for example, in terms of humiliation and harassment for the depicted persons. First, the consequences of the spread of the videos may result in damages to the depicted person's reputation and offensive and sexist comments by online users: sexually explicit deepfakes add a new layer of complexity to what could be used to harass and shame the depicted people.[8]

Second, the dissemination of sexually explicit deepfakes may lead to an invasion of sexual privacy for the depicted person and its consequential harm is profound. Developing future intimate relationships and trust is difficult after one's sexual privacy has been invaded through pornographic deepfakes.[9]

Since pictures of celebrities are readily available across the Internet, it is quite easy for people who have basic technological expertise to create pornographic deepfakes.[10] For example, some pictures of the actress Scarlett Johansson have been used to create deepfake pornographic videos, one of which had been watched over 1.5. million times on a popular website in 2018.[11] The actress expressed all

---

[1] To sum up, Artificial Intelligence (AI) is a machine or a computer program that can perform tasks thought to require human level intelligence.

[2] A. Hauser, M. Ruef, 'Deepfake - An Introduction'. Access online: https://www.scip.ch/en/?labs.20181004 .

[3] Deep learning is a type of AI that imitates the way humans gain certain types of knowledge.

[4] See S. Cole, 'AI-Assisted Fake Porn Is Here and We're All Fucked', MOTHERBOARD (11th December). Access online: https://motherboard.vice.com/en_us/article/ gydydm/gal-gadot-fake-ai-porn.

[5] Several satirical deepfake videos may be found on YouTube. See, for example, Mr Bean talking from White House https://www.youtube.com/watch?v=toyMWF5-byA&list=PL4ikAAfBzP1eUcz_1miGIaT3C7JZIoKsB&index=19 or John Travolta performing in Forrest Gump movie https://www.youtube.com/watch?v=6sUO2pgWAGc&list=PL4ikAAfBzP1eUcz_1miGIaT3C7JZIoKsB&index=8.

[6] *Id.*

[7] D. Harwell, 'Fake-porn videos are being weaponized to harass and humiliate women: everybody is a potential target'. Washington Post (18th December 2019). Access online: https://www.washingtonpost.com/technology/2018/12/30/fake-porn-videos-are-being-weaponized-harass-humiliate-women-everybody-is-potential-target/?utm_term=.4adcb8ad9ad2.

[8] A. Powell, 'Embodied Harms: Gender, Shame and Technology Facilitated Sexual Violence in Cyberspace', (2014), RMIT University, Melbourne.

[9] *Id.*

[10] R. Behun, E. Owens, 'Youth and Internet Pornography: The impact and influence on adolescent development'. 2019.

[11] *Id.*

her frustration coming from the dissemination of that video, declaring that she felt violated and humiliated.[12]

In addition, the technology is available to everyone: there are specific software tools or apps, like FakeApp, which are free on the market and specifically designed to enable people without a technical skills or programming experience create deepfakes.[13] The process is linear: download the software FakeApp, and after that, it is necessary to collect hundreds of pictures of the victim to be superimposed into a video, to feed the photos into FakeApp and run the program; just a relatively well-performing laptop is a structural necessity for being able to produce realistic deepfakes. [14]

Following the steps above with 841 photos of himself, a New York Times journalist used FakeApp and created a convincing deepfake video of his face onto the actor Chris Pratt's body.[15]

Furthermore, as images of the average citizen are becoming easier to get through social media sites, such as Facebook and Instagram, deepfake pornography has begun to impact those who do not hold the celebrity status: a growing number of deepfakes targets people far from the public eye on blogs and private chats calling them colleagues, classmates and friends.[16] The result is a fearsome new way for faceless strangers to inflict embarrassment, distress or shame to colleagues, classmates and friends.[17]

The result is that, according to the last Deeptrace report in 2019, amongst all the different types of deepfake videos, pornographic ones account for a substantial majority (almost 96% of the total videos).[18]

Fig.1.[19] The deepfake footage representing Barack Obama (on the right) together with an original video offers visual illustration of how accurate a deepfake content may seem. This deepfake was created by a group of researchers of Washington University in order to replicate the sounds and cadence of the former US President, given input Obama audio and a reference video.

[12] T. O'Brien, 'Scarlett Johansson says fighting deepfake porn is 'fruitless', The Washington Post, (2019). Access online: https://www.washingtonpost.com/gdpr-consent/?next_url=https%3a%2f%2fwww.washingtonpost.com%2ftechnology%2f2018%2f12%2f31%2fscarlett-johansson-fake-ai-generated-sex-videos-nothing-can-stop-someone-cutting-pasting-my-image%2f.

[13] M. Westerlund, 'The Emergence of Deepfake Technology: A Review' (2019) 9 Technology Innovation Management Review 39. Access online: https://timreview.ca/sites/default/files/article_PDF/TIMReview_November2019%20-%20D%20-%20Final.pdf

[14] A. Dodge, E. Johnstone, 'Using Fake Video Technology to Perpetuate Intimate Partner Abuse', California Partnership to end domestic violence (2019). Access online: https://www.cpedv.org/sites/main/files/webform/deepfake_domestic_violence_advisory.pdf?utm_campaign=site_mail&utm_medium=email&utm_source=webform_submission

[15] K. Roose, 'Here Come the Fake Videos, Too', New York Times (4th March 2018). Access online: https://www.nytimes.com/2018/03/04/technology/fake-videos-deepfakes.html.

[16] *Id.*

[17] *Id.*

[18] H. Ajder, G. Patrini, F. Cavalli, L.Cullen, 'The State of Deepfakes' (2019). Access online: https://deeptracelabs.com/mapping-the-deepfake-landscape

[19] Picture from S. Suwajanakorn, S. Seitz, I. Kemelmacher-Shlizerman 'Synthesizing Obama: Learning Lip Sync from Audio' (2017), 36 ACM Transaction on Graphics. Access online: https://grail.cs.washington.edu/projects/AudioToObama/siggraph17_obama.pdf.

1.2. Problem statement

Notwithstanding the global nature and spread of deepfakes, this thesis is going to focus on the Italian jurisdiction for two main reasons.

First, even though it is a recent phenomenon, a deepfake video depicting the former Italian prime Minister, Matteo Renzi, appeared on a national Italian television channel Canale 5[20]. This video parodied was Renzi's decision to leave the Democratic Party and form his own party. In the parody, Renzi is depicted as discussing the reaction of several politicians, including the former Prime Minister Giuseppe Conte and Italy's president, Sergio Mattarella in an offensive way, calling them "drunk man and old grandfather". The public response to this indicates that people in Italy are susceptible to trust deepfake videos and to react negatively to the individuals depicted: indeed, the result was that this video went viral on social media and became trend topic on Twitter, with users calling Renzi "irresponsible" and insulting him on his official account.[21]

The reported case regarding former Prime Minister Matteo Renzi has spread a highly debated discussion among Italian politicians, intellectuals, journalists and civil society around deepfakes. For example, the former mayor of Rome, Francesco Rutelli and president of ANICA, the Italian National Association of Cinematographic and Audiovisual Industries, promoted a round table to Italian Parliament in December 2019, declaring: "it is essential to raise the awareness of citizens, be less naive in spreading images of themselves that can be used in deepfakes a perverse way and be careful of what we see, raising the level of critical consciousness".[22]

A second reason why the thesis is focusing on the Italian jurisdiction is that, according to the 2013 Survey of Adult Skills, a document of the Organization for Economic Co-operation and Development (OECD) Program for the International Assessment of Adult Competencies (PIAAC), the competence score of Italian adults in literacy is considerably below the average of the OECD countries and the last in the European Union. Notably, adults show an even wider skills gap compared to their peers in other countries.[23] In 2012, around 12 million adults between 25 and 65 scored at the bottom of the PIAAC ranking, while in some parts of the Country seven out of ten adults were discovered to be functionally illiterate.[24] A person who is considered functionally illiterate may be able to read and write simple texts, but show complications interpreting them and distinguishing objective elements from personal opinions.[25] Furthermore, it could be difficult for them to verify the truthfulness of the information, and they are more susceptible to fake news and pictures that have been modified or used in false context.[26] Thus, there could be a potential higher risk in Italy due to the indiscriminate spread of deepfake videos: the difficulties in fact-checking and the lack of critically thinking could lead most

---

[20] S. Venkataramakrishnan, 'Can you believe your eyes? How deepfakes are coming for politics', Financial Times (24th October 2019). Access online: https://www.ft.com/content/4bf4277c-f527-11e9-a79c-bc9acae3b654.

[21] Id.

Matteo Renzi's deepfake video is available at the following link https://www.striscialanotizia.mediaset.it/video/il-fuorionda-di-matteo-renzi_59895.shtml

[22] N. Cottone, 'La manipolazione dei video si presta a crimini gravissimi', Il Sole 24Ore, (24th October 2019). Access online: https://www.ilsole24ore.com/art/deepfake-manipolazione-video-si-presta-crimini-gravissimi-ACqViOv.

[23] A. Schleicher, 'Closing Italy's skills gap is everyone's business', OECD Education and Skills Today, (October 5th 2017). Access online: https://oecdedutoday.com/closing-italys-skills-gap-is-everyones-business/.

See also the Technical Report of the Survey of Adult Skills (PIAAC), 2013 https://www.oecd.org/skills/piaac/_Technical%20Report_17OCT13.pdf

[24] *Id*.

[25] C. Vaccari, A. Chadwick, 'Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty and Trust in News', (2020), Social Media + Society, p. 1–13. Access online: https://journals.sagepub.com/doi/pdf/10.1177/2056305120903408.

[26] *Id*.

of the population to believe the authenticity of the videos and might start spreading them, therefore increasing potential harms.[27]

Because of the predominant amount of pornographic deepfakes online,[28] the focus of this thesis will be on pornographic deepfakes videos. Indeed, the highly realistic nature of the audiovisual material created makes this the ideal vehicle for revenge porn and connected risks such as, invasion of sexual privacy, misogynistic harassment and stalking: a perpetrator may start, endure, or intensify both surveillance and documentation of the depicted individual to obtain the photos in order to create her or his face-superimposed pornographic video.[29] Plus, the offender may obtain the pictures by force, threats and intimidation and the harms of realistic pornographic deepfakes being disseminated and viewed by the public are also significant.[30] Sexually explicit deepfakes are able to achieve new forms of social shaming for the depicted person which goes beyond geographical borders, at vast speeds, to potentially endless audiences.[31]

On one hand, there are no direct laws per se that are specifically tailored to regulate the online dissemination of sexually explicit deepfake videos in Italy by sentencing the perpetrators and facilitating the elimination of the videos; the main problem at stake remains the legal vacuum.[32]

On the other, despite the fact that pornographic deepfakes are not being specifically mentioned in any law, there is an existing framework of criminal law that is already addressed to the harms resulting from the dissemination of pornographic videos in certain contexts.[33]

One of these provisions regards revenge porn, defined as "the distribution of sexually explicit photos or video of people without their permission".[34]The sexually explicit images or video might be recorded by a partner with or without the knowledge and consent of the depicted subject.[35] Therefore, revenge porn and sexually explicit videos comprehend real sexual images of the victims. However, nowadays, in the emerging context of deepfakes, sexually explicit material can be created simply by superimposing the face of the victim into a pornographic video and the line between real and fake remains blurred from the viewer perspective because deepfake technology utilizes real images of the depicted subjects and therefore is not made of false computer generated materials.[36] Thus, despite deepfakes may not be directly covered by revenge porn law, it may be argued that the dissemination of sexually explicit deepfakes could fall within the scope of this provision and that the thesis will examine it more closely.

---

[27] W. Bennett, S. Livingston, 'The disinformation order: Disruptive communication and the decline of democratic institutions', (2018), 33 European Journal of Communication, p.122–139.
See also R. Chesney & D. Citron, 'Deep Fakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics', Foreign Affairs. (Jan./Feb. 2019). Access online: https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war.

[28] D. Harwell, *supra* note 7.

[29] A. Dodge, E. Johnstone E., 'Using Fake Video Technology to Perpetrate Intimate Partner Abuse', (2019), https://www.cpedv.org/sites/main/files/webform/deepfake_domestic_violence_advisory.pdf.

[30] *Id.*

[31] A. Powell, *supra* note 8.

[32] CLUSIT Report on CyberSecurity in Italy, (2020), p. 159-160. Access online: https://d110erj175o600.cloudfront.net/wp-content/uploads/2020/03/Rapporto-Clusit-2020.pdf.

[33] B. Chesney, D. Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy and National Security' (2019) 107 California Law Review. Access online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213954.

[34] D. Citron, 'Criminalizing Revenge Porn', (2014), 49 Wake Forest Law Review, p. 345. Access online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2368946.

[35] *Id.*

[36] *Id.*

Furthermore, revenge porn is not the only phenomenon connected to sexually explicit deepfakes: stalking is defined as "continuative threatening or persecuting behavior which: (1) causes a state of anxiety and fear in the victim(s), or; (2) ingenerates within the victim(s) a motivated fear for his/her own safety or for the safety of relatives, kin, or others associated with the victim him/herself by an affective relationship, or; (3) forces the victim(s) to change his/her living habits".[37] The impact of the dissemination of pornographic deepfake videos may include mental health effects such as depression, anxiety, fear and may lead the victim to change his/her habits.[38]

However, criminal law is not the only legal field where sexually explicit deepfakes may be subsumed: indeed, the creation and dissemination of these types of contents raise personal data protection and right to image violation, as Chapter IV will further describe.

The thesis is going to discuss the harms deriving from the dissemination of sexually explicit deepfake videos in order to outline the level of protection offered by Italian criminal law, data protection law and the right to image to the depicted persons and to assess whether the protection offered is adequate and effective.[39] Indeed, because the thesis cannot assess all the Italian provisions, only the Italian criminal code, the right to be forgotten and the right to image are the chosen provisions in order to offer a picture of the current Italian legislation as much completed and varied as possible, that contains both criminal law and tort law solutions to obstruct the dissemination of sexually explicit deepfake and to restore the victims. From the analysis of the shields offered by criminal law and from the assessment of further protection ensured by data privacy law and copyright law, the thesis will be able to state whether these pieces of legislation are sufficient to effectively protect the depicted persons in sexually explicit deepfakes.

1.3. Research questions and chapters division

All above considered, the thesis will answer the following main research question:

To what extent does the current Italian criminal law framework, the GDPR and the right to image in the Italian context protect individuals depicted in sexually explicit deepfakes?

Consequently, this means answering the following sub-questions:

1.What are deepfakes and what are the main risks associated with sexually explicit deepfake videos for the depicted persons?

2. How does the Italian criminal law framework protect the depicted persons in sexually explicit deepfakes from invasion of sexual privacy, psychological and emotional distress and reputational damages?

3. What are the responses from the application of the right to be forgotten and the right to image in Italy and are these legislative possibilities sufficient to protect the depicted persons in sexually explicit deepfakes?

---

[37] European Parliament, Directorate General for internal policies, The Policy on Gender Equality in Italy, p.20, 2014. https://www.europarl.europa.eu/RegData/etudes/note/join/2014/493052/IPOL-FEMM_NT(2014)493052_EN.pdf.

[38] D. Citron, *supra* note 34.

See also R. Chatterjee 'I Couldn't Talk or Sleep for Three Days': Journalist Rana Ayyub's Horrific Social Media Ordeal over Fake Tweet,', MSN (28th April 2018). Access online: https://www.msn.com/en-in/news/newsindia /%E2%80%98i-couldn%E2%80%99t-talk-or-sleep-for-three-days%E2%80%99-journalist

[39] *Id.*

Chapter II briefly presents the technical background with the explanation of generative adversarial networks, the technology that enables deepfakes. Then it inspects and classify the risks and harms that sexually explicit deepfake videos cause to the depicted persons.
Chapter III examines the Italian criminal law responses to sexually explicit deepfakes. Notably, it will analyze the articles of the Italian criminal code and underline the legal interests protected by these provisions. The chapter discusses whether the values that revenge porn, virtual child pornography, defamation, menace, cyberbullying, cyberstalking protect may be jeopardized and violated by the online dissemination of sexually explicit deepfakes and consequently to discuss whether these articles may apply in cases of non-consensual deepfake pornography.
Chapter IV discusses whether the protection to the depicted persons in sexually explicit deepfakes offered by the Italian criminal code may be ensured, integrated and increased through the implementation of two further and supplementary laws, the data protection and right to image. Then, it will focus on the practical limits of such legislations for a concrete stop of their dissemination.
Finally, Chapter V will assess the conclusions of the thesis, by underlining whether the current Italian criminal law framework is sufficient to effectively protect the depicted persons in sexually explicit deepfake footage. Furthermore, it will briefly present eventual recommendations, such as whether current Italian law needs to be edited or new legislation needs to be implemented.

1.4. Methodology and methods

At the moment, legal academic literature directly dealing with sexually explicit deepfake videos in Italy is almost entirely absent and, in this regard, this thesis plays a pioneering role. Fortunately, taken into account the global nature of deepfakes, profitable reflections are taken from US academic literature, with regards to the legal interests jeopardized and harms caused by the dissemination of sexually explicit deepfakes.
Doctrinal legal research[40] will allow to find the legislation and case law that are connected to sexually explicit deepfakes and can be subsumed under Italian criminal law, data protection and copyright law. Furthermore, doctrinal research[41] will assess the degree and types of harm deriving from the dissemination of these videos for the depicted persons.
In addition, since academic literature cannot be employed in purely doctrinal work, this thesis will rely on interdisciplinary elements: indeed, technology behind deepfakes will be analyzed in Chapter II thanks to the contribution of technical papers.[42]

---

[40] - E. Meskys, A. Liaudanskas, J. Kalpokiene, P. Jurcys, 'Regulating deep fakes: legal and ethical considerations', (2020) 15(1) Journal of Intellectual Property Law & Practice, p. 24-31. Access online: https://doi.org/10.1093/jiplp/jpz167;
- R.A. Delfino, 'Pornographic Deepfakes – Revenge Porn's Next Tragic Act – The Case for Federal Criminalization' (2019) 88 Fordham Law Review. Access online: https://ir.lawnet.fordham.edu/flr/vol88/iss3/2;
'Texas Outlaws 'Deepfakes'—but the Legal System May Not Be Able to Stop Them', Law.com-Texas Lawyers, (11th October 2019). Access online:https://www.law.com/texaslawyer/2019/10/11/texas-outlaws-deepfakes-but-the-legal-system-may-not-be-able-to-stop-them/?slreturn=20200115124016;
- B. Chesney & D. Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy and National Security' (2019) 107 California Law Review 1753. Access online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213954
[41]- D. Citron, 'Sexual Privacy', (2019) Yale Law Journal;
-L. Strahilevitz, 'Consent, Aesthetics, and the Boundaries of Sexual Privacy' (2005) University of Chicago Law School Journal;
-A. Eaton et alia., 'Nationwide Online Study of Nonconsensual Porn Victimization and Perpetration', (2017), 12 Cyber C.R. Access online: https://www.cybercivilrights.org/wp -content/uploads/2017/06/CCRI-2017-Research-Report.pdf.
[42] -M. Westerlund, 'The Emergence of Deepfake Technology: A Review' (2019) 9 Technology Innovation Management Review 39. Access online: https://timreview.ca/sites/default/files/article_PDF/TIMReview_November2019%20-%20D%20-%20Final.pdf;

Finally, doctrinal legal research[43] will be chosen as the main methodology in Chapter IV because any legitimate answer to these research questions is the result of a systematic analysis of data protection and copyright legislation and case law.

The current legal framework in Italy will be further assessed from a socio-legal point of view[44]. Indeed, the thesis will rely on literature taken from the fields of victimology and criminology which elucidates the consequences of sexually explicit deepfake on depicted persons. In addition, this literature clarifies the practical and physiological repercussions that the legislation causes to victims, when it comes to sue the perpetrator and gather evidences.

The methods chosen to answer the main research question and sub questions are academic literature research, legal texts and provisions, case law and news articles. Italian legal texts are the basis to assess which current legislation is applied to sexually explicit deepfakes. The provisions discussed in the thesis are criminal provisions regarding revenge pornography, virtual child pornography, defamation and aggravated defamation, menace, cyberbullying, cyberstalking, the right to image from the Italian Copyright law and the right to be forgotten in the General Data Protection Regulation. Case laws and jurisdiction of Italian Court of last instance (Corte di Cassazione) and Italian Courts offer a wide, detailed and completed picture of the interpretation of the text and laws in order to discuss whether Italian criminal law, data protection law and right to image provisions may be extended and applied in cases of sexually explicit deepfakes. Academic literature research permits to obtain understandings of the technology enabling deepfakes through the contribution of technical papers, the different articles of Italian criminal code, data protection law and right to image and their scope. With all these methods, the research can assess whether the current Italian legislation is able to offer an effective protection to the depicted persons.

- L. Floridi, 'Artificial Intelligence, Deepfakes and a Future of Ectypes' (2018) Philosophy & Technology 31, p. 317-321. Access online: https://link.springer.com/article/10.1007/s13347-018-0325-3.

[43] As Amrit Kharel underlines in his paper 'Doctrinal Legal Research' (February 26, 2018). Access online: http://dx.doi.org/10.2139/ssrn.3130525, "this kind of research deals with studying existing laws, related cases and authoritative materials analytically on some specific matter. With its jurisprudential base on positivism, doctrinal legal research is 'research in law' rather than 'research about law'. Distinguished from literature review, content analysis or historical legal research, doctrinal legal research studies legal propositions based on secondary data of authorities such as conventional legal theories, laws, statutory materials, court decisions, among others."

[44] According to David N. Schiff, in 'Socio-Legal theory: Social Structure and Law' (May 1976). Access online: https://doi.org/10.1111/j.1468-2230.1976.tb01458.x, "for the socio-legal methodology, the analysis of law is directly linked to the analysis of the social situation to which the law applies, and should be put into the perspective of that situation by seeing the part the law plays in the creation, maintenance and/or change of the situation."

Chapter II: Sexually explicit deepfakes

2.1. Introduction

The main focus of this chapter is on sexually explicit deepfake. Indeed, before moving to the analysis of legal responses that protect the interests and values violated by this type of deepfakes, it is necessary to understand clearly what sexually explicit deepfakes are and what kind of benefits and harms are connected to them. The whole chapter is centered according to the perspective of the depicted persons in sexually explicit deepfake videos. In order to achieve this goal, paragraph 2.2 the research analyzes the technical background of deepfake technology and how it can be utilized to produced sexually explicit deepfakes. The benefits of deepfake technology are discussed in paragraph 2.3. On the other hand, paragraph 2.4 will exclusively focus on the issues and harms associated to the dissemination of sexually explicit deepfake videos for the depicted persons, as this is the main focus of the research. Finally, paragraph 2.5 contains a short conclusion. The technical background of deepfake technology together with its benefits aim at offering a more complete overview of the origin and the use of this footage in the field of simultaneous interpretation and movies. However, the core analysis of this chapter refers to the harms related to sexually explicit deepfakes: this examination will help the research to restrict the typologies of damages according to the perspective of the depicted persons, to classify them and to state whether there are significant differences between harms caused by a real pornographic video and harms caused by deepfake sexually explicit contents.

2.2. Technology enabling deepfakes: the neural networks and the generative adversarial networks (GAN)

The creation of deepfakes relies on two typologies of artificial intelligence: neural networks and generative adversarial networks (GANs).[45]

Neural networks function in a way comparable to the human brain because both the brain and neural networks are able to process information in a faster and more accurate way as they are exposed to and learn from more and more information. Indeed, the more the human brain is exposed to examples of some actions, such as how to kick a ball or the lyrics of a new song, the faster and more accurate the brain is able to replicate it.[46] Neural networks use this same concept: they take data and divide it into small pieces (bites), then analyze the rapports between those pieces in order to understand what these data are.[47] To offer an example, through neural networks, the machine looks at two pictures of dogs and detects that they are diverse individual animals, but both dogs; then it memorizes the mathematic formula for the idea of a dog: four legs, plus triangular ears, plus a shape like a snout, plus a tail, plus fur. Equals a dog.[48]

However, neural networks represent only half of the path and without GANs, deepfakes would not be as realistic as they are. Indeed, neural networks need to receive realistic input data and images from GANs in order to memorize them. GANs are the combination of two neural networks in adversarial roles: the first neural network, the so-called generator, creates the fake video or audio by

[45] D. Yadav, S. Salmani, 'Deepfake: A Survey on Facial Forgery Technique Using Generative Adversarial Network', (2019), International Conference on Intelligent Computing and Control Systems (ICCS), p. 852-857.

[46] K. Tero, T. Aila, S. Laine, J. Lehtinen. 'Progressive Growing of GANs for Improved Quality, Stability, and Variation' (2017).

[47] D. Güera, E. J. Delp, 'Deepfake Video Detection Using Recurrent Neural Networks', 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS). (27-30 November 2018). Access online: https://ieeexplore-ieee-org.tilburguniversity.idm.oclc.org/abstract/document/8639163.

[48] *Id.*

attempting to duplicate the dataset it is being fed, i.e. the pictures of the depicted person.[49] Then, both the original dataset, and the newly created deepfake, are fed into a second neural network, known as the discriminator, that chooses which videos in the dataset are real.[50] When the discriminator is able to recognize the deepfake, the generator can then "learn" how the discriminator determined the fake and correct whatever error was made; it understands the differences between the real video and the previous fake attempt in order to improve its performances and reproduce a video or audio which are closer to the original fed in the dataset.[51]

To come back to the previous practical example, the neural network takes the "dog formula" and applies it to create what it thinks the answer for "dog" is, based on all the dogs its creator has shown it in the past.[52] The second network has also been trained on pictures of real dogs; it judges whether what the first network came up with is a real dog or not.[53] That second network doesn't know that a fake dog is fake, and it simply determines whether what it sees is a real dog, according to its understanding, or not.[54]

In order to create deepfakes, the GANs are fed datasets of the video that will be depicted, that may be a movie, a sexually explicit picture or a recording of speech. In addition, the GANs are also fed datasets containing images, videos or voice recordings of the person who will be depicted in the video, picture or voice recording.[55]

Thus, the more pictures and videos of a person are exposed to a neural network, the more precisely it is able to reproduce gestures, sounds, and facial expressions of that person when creating a deepfake video;[56] if a dataset comprehending every public statement made by the former president of the United States of America Donald Trump is fed through a neural network, the network will then be able to generate a video or an audio that is almost indistinguishable from the real video and audio.[57]

This happens because deepfakes designers do not only operate in terms of categories recognition: once the facial gestures of Mr. President Donald Trump have been trained and created, they are able to combine, cut and fit perfectly them into a random pornographic video, as he is being part of a sexual intercourse. Therefore, the fact that there are not real pornographic images or videos of Mr. Donald Trump is not necessary because it is possible to create them.[58]

The outcome is a precise and invasive type of digital manipulation that is much more developed and precise than the face-swapping filters which may have been common on social medias, such as Instagram and Snapchat: the neural networks manipulate not only facial expressions but also numerous movements including head positions and rotation, eye gaze and blinking. This manipulation is also invasive because the creator takes away a victim's control of his/her face, using

---

[49] T. Kirchengast, 'Deepfakes and image manipulation: criminalization and control', (2020), 29 Information & Communications technology law 3, p. 308–323. Access online: https://doi.org/10.1080/13600834.2020.1794615.

[50] *Id.*

[51] *Id.*

[52] D. Güera, E. J. Delp, *supra* note 47.

[53] *Id.*

[54] *Id.*

[55] *Id.*

[56] S. Dack, 'Deep fakes, fake news and what comes next', (2019) Henry M. Jackson School of International Studies - University of Washington. Access online: https://jsis.washington.edu/news/deep-fakes-fake-news-and-what-comes-next/#_ftn8.

[57] B. Marr, 'The Best (And Scariest) Examples Of AI-Enabled Deepfakes', Bernard Marr Blog (2020). Access online: https://bernardmarr.com/default.asp?contentID=1927.

[58] *Id.*

it for something he/she never wanted.[59]The fake videos may have all the types of contents, including pornographic.[60]

2.3. Benefits of deepfake technology

Deepfake technology shows several benefits in the field of entertainment and translations.

First, there are different artistic benefits associated with the use of this technology. It offers artists, designers and creators the chance to make realistic content where public figures such as politicians can be satirized, parodied and constructively criticized.[61] In addition, deepfake technology can be used to produce special effects in movies and TV shows.[62]

Second, the technology can overpass the distances deriving from language comprehension, for example during meetings or videoconferences by translating the speech and adjusting the movements of the face and lips in order to be harmonized with the translated language. In this way, everyone seems to be speaking the same language, which makes communication easier, faster and more natural. This is not only useful for companies and non-governmental organizations but also for several types of online interactions: indeed, deepfake technology can also transform promotion and advertising in significant ways.[63]

For example, deepfake technology was used in the context of malaria awareness campaign titled "Malaria must die, so millions can live". More specifically, a deepfake video representing English football star David Beckham speaking nine languages, including Spanish, Arabic, Hindi and Mandarin and encouraging more people to raise awareness of the disease.[64]

2.4 Harms of deepfake technology

Besides the different benefits that, on a general level, deepfake technology offers, there are also different harms and damages that sexually explicit deepfake videos can cause. These harms are likely to produce effects on different levels, namely on the individual and personal sphere of the depicted persons and on the level of external relation with society. The depicted persons may be public figures or even private persons, including minors.

Comprehending the consequences of sexually explicit deepfakes requires a deep analysis of the borders between the virtual and the real.[65] But most importantly, understanding the harm caused by deepfakes inevitably includes going beyond a strict focus on the technology to comprehend the approaches and behaviors, such as misogyny and sexism, that drive their creation.[66] In other words, Citron underlines that the harm of fake pornography is not caused by the realism of the representation; according to her "whether the representation is text-based, picture-based, or in video form such as deepfakes, and even when the fake pornographic representation is neither exactly real nor exactly make-believe the harm is nonetheless profoundly, compellingly, and emotionally true".[67]

In the following paragraphs, the research and the analysis of the damages caused by sexually explicit deepfake videos amplify and confirm Citron's assumption by reporting the typologies of harms and

---

[59] S. Dack, *supra* note 56.
[60] *Id.*
[61] B. Chesney B, D. Citron, *supra* note 33.
[62] *Id.*
[63] *Id.*
[64] S. Barr, 'David Beckham appeals for end to malaria by 'speaking' in nine languages', the Independent (9th April 2019). Access online: https://www.independent.co.uk/life-style/health-and-families/david-beckham-malaria-must-die-campaign-disease-nine-languages-a8861246.html.
[65] A. Waldman, 'A Breach of Trust: Fighting Nonconsensual Pornography', (2017) 102 Iowa Law Review 709, p.10.
[66] *Id.*
[67] *Id.*

by concluding there are not significant differences between a real pornographic video and a deepfake video in terms of harms caused to the depicted persons.

2.4.1 Harms deriving from virtual child pornography

Because deepfake technology is used to create realistic pornographic videos and since these videos are likely to be largely spread on the internet, sexually explicit deepfakes are in the realm of sexually exploitative cybercrimes and are examples of image-based sexual abuses, such as virtual child pornography.

Indeed, as Eneman *et alia* pointed out, "virtual child pornography refers to computer generated images, drawings, paintings and cartoons portraying sexual representation of children: they are created wholly through computers and does not involve the physical abuse of real children but nevertheless raise important legal and ethical issues".[68] It thus may rely on artificial intelligence networks and be based on deepfake technology.

The real danger deriving from virtual child pornography is the possibility that molesters utilize these types of contents to rouse their own desires and fuel their imagination for sexual intercourses with minors. Indeed, viewing virtual child pornography may sharpen the hunger of the perpetrator and may be precursory to sexual acts with children.[69]

The risk is that the more often the harasser looks on child pornography, including virtual child pornography generated via deepfake technology, the more he or she becomes insensitive to the aberration of his or her behavior and may convince himself or herself that these sexual fantasies are normal.[70]

Then, when mere graphic stimulation no longer satisfies him, the molester may often move to harassing minors in real life.[71]

To sum up, virtual child pornography is a criminal instrument utilized to seduce and control minors and make sexual intercourses between adults and children seem normal. This is the reason why virtual child pornography is not only an issue connected to the abuse of a named minor, but it regards the sexual depiction of minors *per se* and, as the American attorney John Waters underlined "any use of a child - or the idea of a child - to obtain sexual gratification represents, in principle, an attack on all children".[72]

2.4.2. Revenge pornography

It is not just children who may face significant harm from fake pornographic depictions of themselves. Indeed, sexually explicit deepfake footages are generally created and spread without the consent of the individuals depicted and may be consequently subsumed under revenge pornography or non-consensual pornography crimes.[73]

---

[68] M. Eneman, A. Gillespie, B. Stahl, 'Criminalising fantasies: the regulation of virtual child pornography', (2009), Proceedings of the 17th European conference on information systems. Access online: https://www.researchgate.net/profile/Bernd_Stahl/publication/265357703_CRIMINALISING_FANTASIES_THE_REGULATION_OF_VIRTUAL_CHILD_PORNOGRAPHY/links/543186210cf277d58e982ac8/CRIMINALISING-FANTASIES-THE-REGULATION-OF-VIRTUAL-CHILD-PORNOGRAPHY.pdf.

[69] J. Waters, 'Real dangers of virtual child porn', (27th January 2003), The Irish Times. Access online: https://www.irishtimes.com/opinion/real-dangers-of-virtual-child-porn-1.346757 .

[70] *Id.*

[71] *Id.*

[72] *Id.*

[73] A. Flynn, N. Henry, 'Image-Based Sexual Abuse: An Australian Reflection in Women & Criminal Justice', (2019). Access online: https://www-tandfonline-com.tilburguniversity.idm.oclc.org/doi/full/10.1080/08974454.2019.1646190.

Revenge porn is defined as the act of "disclosing a private, sexually explicit image to someone other than the intended audience without the consent of the involved individuals*"* and it refers to two crucial conducts: the creation, taking, or recording of naked or sexual images and the sharing or dissemination of these types of images.[74]

It defines the dissemination of authentic sexually explicit photos or videos without the subject's consent[75]. Indeed, partners in an intimate and stable relationship may consensually share photos or videos that one partner later share in revenge against the other.[76]

It is likely that people would have many pictures of their partner and therefore potentially own lots of material to produce sexually explicit deepfakes, together with partner's picture posted on social media.

However, even strangers can take and utilize revenge porn pictures and videos through hacking or theft of a smartphone, tablet or laptop.[77] Hackers may post these materials on the internet with or without the victim's personal and sensitive identifying information.[78] Revenge porn is also indicated to more largely as "nonconsensual pornography", that comprehends sexually explicit pictures or videos recorded without the individual's consent, such as recordings through hidden cameras.[79]

2.4.3 Psychological and emotional harms deriving from revenge pornography and sexually explicit deepfakes

Both sexually explicit deepfakes and revenge porn have problematic similarities.

First of all, they include the nonconsensual dissemination of sexually explicit material: victims of revenge porn do not consent to public distribution of their sexual images and videos, and similarly, in most cases victims of deepfakes do not agree to superimposition of their face onto the body of an individual engaging in sexual acts.[80] Thus, revenge porn and deepfakes both violate people's legitimate expectations that the distribution of sexual explicit materials is funded on consent.[81] Both revenge porn and pornographic deepfakes can determine long-term effects for victims and can produce analogous emotional and psychological harms.[82] By way of illustration, the Cyber Civil Rights Initiative, a civil rights group fighting against revenge porn and sexually explicit deepfakes and promoting awareness for victims, conducted a survey with 1,606 responses, 361 of whom self-declared as victims of revenge porn and 67 victims of photoshopped pornographic pictures. The survey found that "90% of victims were women; 57% of victims reported that an ex-boyfriend posted the material; 59% reported that the material included their full name; 93% of victims reported suffering from emotional distress; 82% reported a social, occupational, or other impairment due to the material; 49% reported that they were harassed or stalked online because of the material, while 30% said they were harassed or stalked outside of the Internet by online users who saw the material; 8% reported quitting a job or dropping out of school; 3% have legally changed their names; 54%

[74] R. Delfino 'Pornographic deepfakes: the case for federal criminalization of revenge porn's next tragic act' (2019) Fordham Law Review 887. Access online: https://ir.lawnet.fordham.edu/flr/vol88/iss3/2.
[75] *Id.*
[76] *Id.*
[77] S. Greengard, 'Will deepfakes do deep damages?' (2020), 63(1) Communications of the ACM, p.17-19. Access online: https://dl.acm.org/doi/fullHtml/10.1145/3371409.
[78] *Id.*
[79] *Id.*
[80] D. Citron, *supra* note 34.
[81] *Id.*
[82] *Id.*

worried about their children seeing the explicit material online and 51% have had suicidal thoughts due to being a victim of revenge porn".[83]

Several scholars have agreed that victims feel the consequences of the dissemination of their sexual videos on a social level: losing a job or future potential for a job, creating a completely new identity to escape harassment, and losing current or future friend or romantic partner. In addition, victims also feel the consequences on a private and intimate level: fearing for children or families; facing depression, anxiety, and post-traumatic stress disorders; or even committing suicide.[84]

Thus, revenge porn not only damages a person's affecting well-being but also makes risks of relevant professional, academic and even physical injury, including abuses and stalking.[85]

Chesney and Citron underline that when victims find out that their faces have been superimposed into pornographic images and videos, the psychological pressure can be considerably damaging[86]. And it is not important what the creator intended to do with this deepfake: the depicted persons can feel a wide variety of emotions from being terrorized, to being humiliated or even psychologically abused.[87]

Fake porn videos treat women like sexual objects forcing them into non-consensual virtual sex and a more chilling effect of deepfake porn videos is that they can also "transform rape threats into a terrifying virtual reality. They send the message that victims can be sexually abused at whim".[88]

The abuses may also be online through deepfakes and can entail intentional damages of victim's reputation by spreading malicious gossip, rumors or photos. In addition, deepfakes are often disseminated online with the name of the depicted persons and this potentially lets everyone to search information about them, helping potential stalkers to harass the victim continuously.[89] Indeed, chronicles are full of examples regarding talkers continuously follow a person, generally a celebrity, on the basis of his/her online contents and it is not possible to exclude that this may happen to depicted persons in pornographic deepfakes.[90]

Furthermore, like revenge porn, sexually explicit deepfakes spread women objectification.[91]

Scholars have shown that sexually explicit media tend to encourage women's role as sex objects for male pleasure.[92]Several videos and images analyses have regularly demonstrated that women are often represented as sexual objects in pornographic contents[93]. Notably, a content analysis of bestselling and most-viewed pornographic videos has found that more than two out of ten scenes

---

[83] K. Gabriel, 'Feminist revenge: seeking justice for victims of nonconsensual pornography through revenge porn reform' (2019), 44 Vermont Law Review. Access online: https://lawreview.vermontlaw.edu/wp-content/uploads/2020/07/06-Gabriel.pdf.

[84] *Id.*

[85] *Id.*

[86] B. Chesney, D. Citron, *supra* note 33.

[87] *Id.*

[88] *Id.*

[89] R. Delfino, *supra* note 74.

[90] In this regard, see T. Taylor, 'Extreme celebrity stalking in the digital age', Face Magazine (18th October 2019). Access online: https://theface.com/culture/celebrity-stalking-harry-styles-taylor-swift-ena-matsuoka-miley-cyrus.

[91] S. Cole, 'Deepfakes Were Created as a Way to Own Women's Bodies—We Can't Forget That', Vice Magazine (19th June 2018). Access online: https://www.vice.com/en_ca/article/j5kk9d/deepfakes-were-created-as-a-way-to-own-womens-bodieswe-cant-forget-that-v25n2.

[92] P. Wright, E. Donnerstein, 'Sex Online: Pornography, Sexual Solicitation, and Sexting' (2014), 25(3) Adolescent Medicine: State of the Art Reviews, p. 574-589.

[93] L. Vandenbosch, J. Van Oosten, 'The Relationship Between Online Pornography and the Sexual Objectification of Women: The Attenuating Role of Porn Literacy Education' (2017) 67 Journal of Communication, p. 1015-1036. Access online: https://academic.oup.com/joc/article-abstract/67/6/1015/4753857?redirectedFrom=fulltext.

showed male ejaculation on female's body or face[94] and such representation of male orgasm is considered to embody women objectification.[95] In this regard, the American journalist Samantha Cole defined deepfakes as "a mode for men to have their full and complete, fantastical way with women's bodies".[96]

To conclude, the following harms for the depicted persons which are reported in the context of revenge porn, may still be present even if the content is a deepfake:

- emotional distress derived from the invasion of sexual privacy such as fear, humiliation, body objectification, or, in the most extreme cases, suicidal thoughts;
- social or occupational impairment derived from the libel given to the depicted persons, which my lead to lack of jobs, trust and social interactions;
- harassment and online stalking because the wide audience of deepfakes can participate in harming the victim with comments, views, interactions and sharing.

2.4.4 Sexually explicit deepfakes and invasion of sexual privacy

The dissemination of sexually explicit deepfakes video leads to several kind of harms for the depicted person: online users, and women in particular, have been targets of the non-consensual pornography and image abuses.[97]

Danielle Citron is probably the scholar who mainly offers a possible location for the harm. She spreads the notion and idea of 'sexual privacy', underlining that it determines a significant impact to individuals, groups, and entire society.[98] She recognizes sexual privacy as the basis for women and men identification because sexual privacy let us to be who we want to be, and to equality, because imposed public visibility of our intimate acts, thus the invasion of sexual privacy, is likely to lead to marginalization and frustration.[99] Citron clearly identifies the harm of non-consensual fake pornography as a harm to sexual privacy: deep fake sex videos involve an invasion of sexual privacy by exercising dominion over individuals' intimate identities.[100] They reduce individuals to their genitalia and breasts, they destabilize the ability to show identities with integrity, attaching them with damaged ones and, to conclude, they are an outrage to individuals' sense that their intimate personalities are their own and are not made public.[101]

Therefore, according to Citron, "the harm of sexual privacy invasions is profound", undermining the growth of personal identity by an agency over their intimate lives.[102] These types of invasions create a scenario allowing the only sexual aspect of one's self to eclipse all other aspects, in terms both of how depicted persons look at themselves and how they are seen and judged by others, decreasing them to mere sexual objects to be exploited and exposed.[103] The latter description is likely to fit properly with the experiences and thoughts expressed by targets of tech-facilitated violence and abuse, including the harm of non-consensual fake pornography.[104]

---

[94] A. Bridges, R. Wosnitzer, E. Scharrer, C. Sun, R. Liberman, 'Aggression and Sexual Behavior in Best-Selling Pornography Videos: A Content Analysis Update", (2010), 16(10) Violence against women, p.1065-85

[95] *Id.*

[96] S. Cole, see 91.

[97] A. Eaton et alia, *supra* note 41.

[98] D. Citron, 'Sexual Privacy' (2019) Yale Law Journal.

[99] *Id.*

[100] *Id.*

[101] *Id.*

[102] *Id.*

[103] D. Harris, 'Deepfakes: False Pornography is Here and the Law cannot Protect You' (2019) 17 Duke Law & Technology Review 99. Access online: https://scholarship.law.duke.edu/dltr/vol17/iss1/4/.

[104] *Id.*

In line with this thought, Cole evidences that "deepfakes were created as a way to own women's bodies"[105]. This is a crucial point, and it is fundamental to put this notion in contrast with the level of reality and even unrealistic misogynistic representations are likely to determine social and emotional damage to depicted person.[106] Producers and consumers of fake pornography could try to argue that they do not cause harm because the videos are not real, but for the targets whose faces are the ones being superimposed, that argument is absolutely debatable, since the intention is clear and evident.[107] Moreover, the objectification and ownership of the body is likely to be analyzed according to a double perspective: indeed, notwithstanding porn actresses and actors whose scenes are used are not the direct subjects of this abuse, the reproduction of their bodies doesn't reduce the sense of violation and frustration that porn industry members feel once they have realized the phenomenon, or the fears they have about how this technology could be used to harass them.[108] For example, porn actress Sydney Leathers was intimately familiar with what it feels like to have her work used to harass another woman: indeed, in January 2019, a bathtub selfie that she had posted started to circulate online, repackaged as a naked photo of American congressmember Alexandria Ocasio-Cortez.[109]
For Leathers, the experience was deeply upsetting. As she reported to medias, she felt violated, upset and guilty, notably she felt to be part of the harassment of another women particularly since Ocasio-Cortez is a politician she likes and respects.[110]

2.4.5 Sexually explicit deepfakes and reputational damages

Even whether sexually explicit deepfakes will be discovered by the depicted person, it might be too late for the victims.[111] Apart from the inflicted psychological damage and online abuses, sexually explicit deepfakes can cause individuals to lose their jobs or altogether to terminate any hope for their current or future careers.[112] Indeed, the post-truth climate that we live in only increases the chances of such deepfakes to be distributed by thousands of online users regardless of their truth, producing irreparable reputational damage to individuals involved in the process.[113] And once out there on the World Wide Web shared by thousands and thousands of people, these deepfakes will be hard if not impossible to remove.[114] In 2018, Google added involuntary synthetic pornographic footage to its ban list; each user is thus able to ask to block in the search engine the results that falsely show them involved in a sexually explicit situation. However, this report function intervenes only when the pornographic deepfake has been already created and spread online and it only blocks the search engine results, but it is not effective when the dissemination of this kind of materials is done via alternative channels, such as text and voice messaging apps like Telegram and Whatsapp or via email.[115]
Meskys *et alia* evidence that, without question, the mere acts of falsely placing someone's face in an pornographic video without his or her consent and the act of spreading this video online seriously

---

[105] S. Cole, 'AI-Assisted Fake Porn Is Here and We're All Fucked', MOTHERBOARD (2017). Access online: https://motherboard.vice.com/en_us/article/gydydm/gal-gadot-fake-ai -porn.
[106] *Id.*
[107] *Id.*
[108] *Id.*
[109] L. Alpatrum, 'Deepfake Porn Harms Adult Performers, too', Wired Magazine, (15th January 2020). Access online: https://www.wired.com/story/deepfake-porn-harms-adult-performers-too/.
[110] *Id.*
[111] D. Harris, *supra* note 103.
[112] R. Delfino, *supra* note 40.
[113] *Id.*
[114] *Id.*
[115] *Id.*

harm the reputation of the depicted person, without regard to the truth of the video, as to lower him in the estimation of the entire or part of his community or to deter third persons from associating or dealing with him.[116]

For example, it is interesting to report the story of Noelle Martin, an 18-year-old law student who did a reverse Google image search out of curiosity, uploading a picture of herself to see where else it was on the internet and finding hundreds of explicit images of her face photoshopped and superimposed onto the bodies of porn actresses engaged in sexual acts.[117] As she reported to media, she was so ashamed, humiliated, embarrassed, frightened and paranoid of what this meant for her future, her goals, her dreams and her career.[118] When talking about her first reaction to seeing the fake porn video about herself, Noelle said it was a destructive experience and that she just couldn't show her face.[119] She was able to call herself a journalist or a feminist but, in that moment, she just couldn't see through the humiliation because she felt so embarrassed: the entire country was watching a porn video that claimed to be her and she just couldn't bring herself to do anything.[120] Moreover, hating comments portraying her as "prostitute", "attention-seeking" and "garbage" started to spread online, even once she decided to report her story to medias.[121] This leads to a significant impact on her name, her narrative and her reputation both online and in real life: for example, one picture of her accepting a Young Achievers prize was doctored to show her holding a pornographic DVD instead of a certificate, printed and distributed in her university.[122]

Potentially, the whole country had access to a deepfake porn. The higher the visibility of the story, the more convincing it is among users who encounter it.[123] Indeed, the fact that today news are spread in an algorithmic manner on social media platforms, has changed the way in which things become visible to our society.[124]

Moreover, if certain misinformation or fake news targeting an individual becomes a viral phenomenon, it only gains more visibility and thus potentially causing even further harm.[125] As Medrán underlined, "it is not only high visibility that makes these videos believable: it is people's susceptibility to being easily swept away by rumors, lies and misinformation which reinforce their pre-existing beliefs and opinions that pose a real threat".[126]

The reputational damages show themselves in several ways. People may judge the victim on the basis of the presence of their nude contents online and everybody can see and share them, even whether this video is fake. The dissemination of sexually explicit footage may produce consequences on relationships because actual or future partners may not feel comfortable with the presence of nude videos of their partner on the Internet. In addition, this can cause dangers to victims' employment research: companies may reject to hire a candidate because the results on search engines of the

---

[116] E. Meskys, A. Liaudanskas, J. Kalpokiene, P. Jurcys, *supra* note 40.
[117] K. Melville, 'The insidious rise of deepfake porn videos and one woman who won't be silenced', ABC news Australia. (30th August 2019). Access online: https://www.abc.net.au/news/2019-08-30/deepfake-revenge-porn-noelle-martin-story-of-image-based-abuse/11437774
[118] *Id.*
[119] *Id.*
[120] *Id.*
[121] *Id.*
[122] *Id.*
[123] A. Medrán, 'In the kingdom of post-truth, irrelevance is the punishment. The Post-truth Era: Reality vs. Perception'. (2017) p. 33-35.
[124] *Id.*
[125] *Id.*
[126] *Id.*

applicant's name contain nude contents of the applicant, such as sexually explicit deepfake videos.[127] Indeed, search results are particularly relevant to employers. According to Fertik 75% of the employer companies actively search prospect workers online and more than 70% rejected to hire somebody on the basis of the results they found on the Internet.[128] In addition, recruiters use to dig really deep during their searches, through social media platforms, shopping profiles, online gaming websites and auction sites, thus they are more likely to find potential sexually explicit deepfakes of the victim.[129]

2.5 Conclusion

This chapter analyzed deepfake technology and its benefits, then focused on the damages of pornographic deepfakes and concluded that there are not significant differences between a real pornographic video and a deepfake video in terms of harms caused to the depicted persons.

The depicted persons may be public figures and private citizen, with a specific focus on female and children condition and the focus in this research is particularly on the use of deepfake technology for the creation of sexually explicit footage because the dissemination of this type of videos or pictures generates several specific issues.

Indeed, there are a variety of damages that can occur: the harms that depicted people can suffer due to the dissemination of sexually explicit deepfakes are psychological and emotional ones deriving from the stigma on sexual images, damages deriving from the invasion of the sexual privacy of depicted person, reputational damages and economic damages, such as the difficult to find a job and maintain social relationships.

This distinction may sometimes overlap whether the depicted person is a public figure or a private citizen. In addition, damages may affect both the individual sphere and the external relation with society of the depicted persons.

While psychological and emotional distress and invasion of sexual privacy are clearly part of the individual sphere, reputational and economic damages may affect both the public and private sphere of the depicted persons.

Furthermore, when a minor engaging sexual activity is depicted in a deepfake video the danger of normalize sex with children is in place in molesters' fantasies and this may lead to sexual harassment toward children in real life.

[127] M. Fertik, 'Your Future Employer Is Watching You Online. You Should Be, Too' (2012) Harvard Business Review. Access online: https://hbr.org/2012/04/your-future-employer-is-watchi.
[128] *Id.*
[129] *Id.*

Chapter III: Italian criminal law responses

3.1 Introduction

Chapter II has analyzed the risks and harms associated with the dissemination of sexually explicit deepfakes and has showed that these harms are common both in real pornographic footage and in deepfake videos. The risks for the depicted person are categorized into unauthorized invasion of sexual privacy, psychological and emotional distress and reputational damages. This chapter examines the legal response that the Italian criminal law framework offers to protect the depicted persons and detects the legal interests that the provisions aim to guarantee in order to underline the strengths and weaknesses of Italian criminal law responses in the prevention of the above-mentioned risks. Indeed, the Italian Criminal Code contains different provisions that may be applicable to the dissemination of sexually explicit footage which will be examined in this chapter.

Paragraph 3.2 will analyze revenge pornography, paragraph 3.3 virtual child pornography, paragraph 3.4 defamation and its aggravated form, paragraph 3.5 menace, 3.6 cyberbullying, 3.7 cyberstalking. Finally, a short conclusion will be synthesized in paragraph 3.8.

All the paragraphs will detect the precise legal interest to be protected by the criminal law provision. As Citron and Franks underlines, "legally protected interests, or virtues, are socially approved values and objects that are safeguarded by criminal law: interests can be private or public and range from life, body and limb, sexual integrity and identity, privacy, personal data, property, national security, a country's monetary system, or health system, etc".[130] This chapter will analyze how the Italian criminal law framework defends the depicted persons in sexually explicit footage in order to categorize in which Criminal law provision the legal interest of sexual privacy, psychological integrity and reputational sphere find protection.

3.2. Revenge pornography

The Italian Criminal law framework includes a provision that criminalizes revenge pornography: article 612 ter.

Until 2019, Italy has not implemented any specific laws, bills, decree or Criminal Code articles that regulate and criminalize revenge pornography. In 2016, there was a shocking revenge pornography case in Italy that ended with the suicide of the victim Tiziana Cantone, a 31-year-old women who could not escape the notoriety produced by the sex tape she featured in and who did not find legal recourse under the existing Italian law.[131] The first response to the vacuum in Italian Criminal law was through the so called "Cyberbullying Act", passed in 2016, which criminalizes the act of posting insults or defamatory messages concerning a minor online; blackmail them on the internet; or, steal their identity.[132]

In July 2019, Italy adopted a new substantive legislative act, the law 19 July 2019 no. 69 named "Amendments to the Criminal Code, the Criminal Procedure Code and other provisions on the protection of domestic and gender-based violence victims, also known as the "Red Code" ("Codice Rosso" in Italian language) in order to regulate several and varied types of sexual violence, with

[130] D. Citron, *supra* note 34.

[131] See 'Tiziana Cantone: Suicide following years of humiliation online stuns Italy', BBC News, (2017). Access online: https://www.bbc.com/news/world-europe-37380704.

[132] F. Colleti 'Revenge porn: the concept and practice of combatting nonconsensual sexual images in Europe' (2017) European Master's Degree in Human Rights and Democratization - University of Latvia.

specific regard to women's condition.[133] Amongst the other amendments, the Red Code bill modified the Italian Criminal Code and added to its provisions the article 612 ter, named "Illicit dissemination of sexually explicit images and videos" which regulates revenge pornography. This article is made up of four paragraphs.

The first paragraph of the new article[134] states that "anyone sending, donating, selling, posting or distributing images or videos, that are allegedly private, depicting a person with explicit sexual content, after recording or stealing them and without the consent of that person, shall be punished with imprisonment for one to six years and with a fine for 5000 and 15000 euros.[135]

The second paragraph of this article imposes the same penalty to those who have received or otherwise obtained the sexually explicit pictures or videos, and who send, donate, sell, publish or distribute them without the consent of the depicted persons in order to cause them harm.[136]

Paragraph three increases the penalties in three cases: whether the spouse of the depicted person commits the act, even whether legally separated or divorced; whether the dissemination is committed by a partner who is actually having or has had an intimate relationship with the depicted person; and whether the dissemination is done through computer or electronic means.[137]

To conclude, the fourth paragraph increases the penalty whether the act is committed against a person who is physically or mentally weak or against a pregnant woman.[138]

Many scholars agree that the Red Code has drastically improved the quality of criminal responses to revenge pornography in Italy and that the new article 612 ter increases the protection against the violation of invasion to intimate and sexual private sphere of the depicted person.

As Caletti underlines, "with the new article embodied in the Criminal Code, Italy has become the country in continental Europe with the most severe and serious approach to revenge pornography".[139]

In addition, imprisonment up to six years shows that Italy looks at revenge pornography as a serious sexual crime and protects the sexual integrity and sexual privacy of the individuals.[140]

Furthermore, Amore evidences how the inclusion of the "non-consensual" dissemination of sexually explicit contents is justified by its direct connection with freedom and confidentiality of sexual life to which this conduct seem to threaten.[141] Indeed, whether the depicted person agreed to expose her

---

[133] M. Šepec, 'Revenge Pornography or Non-Consensual Dissemination of Sexually Explicit Material as a Sexual Offence or as a Privacy Violation Offence' (2019) 13(2) International Journal of Cyber Criminology. Access online: https://www.cybercrimejournal.com/MihaSepecVol13Issue2IJCC2019.pdf.

[134] See the Italian Official Journal, https://www.gazzettaufficiale.it/atto/serie_generale/caricaArticolo?art.progressivo=0&art.idArticolo=10&art.versione=1&art.codiceRedazionale=19G00076&art.dataPubblicazioneGazzetta=2019-07-25&art.idGruppo=0&art.idSottoArticolo1=10&art.idSottoArticolo=1&art.flagTipoArticolo=0

[135] G. M. Caletti, 'Il testo del disegno di legge "Codice Rosso" (Text on the "Codice Rosso" legislatve bill)' (2019) Diritto Penale Contemporaneo. Access online: https://archiviodpc.dirittopenaleuomo.org/d/6622-il-testo-del-disegno-di-legge-codice-rosso-revenge-porn-costrizione-o-induzione-al-matrimonio-defor.

[136] *Id.*

[137] *Id.*

[138] *Id.*

[139] G. M. Caletti, 'Sexual Freedom and Privacy in the Age of Internet. Article 612-ter of the Italian Criminal Code and Criminalisation of Non-consensual Pornograph' (2019) Rivista Italiana di diritto e procedura penale. Access online:https://www.academia.edu/43533049/LIBERT%C3%80_E_RISERVATEZZA_SESSUALE_ALL_EPOCA_DI_INTERNET_L_ART_612_TER_C_P_E_L_INCRIMINAZIONE_DELLA_PORNOGRAFIA_NON_CONSENSUALE_Sexual_Freedom_and_Privacy_in_the_Age_of_Internet_Article_612_ter_of_the_Italian_Criminal_Code_and_Criminalisation_of_Non_consensual_Pornography>.

[140] *Id.*

[141] N. Amore, 'La tutela penale della riservatezza sessuale nella società digitale. Contesto e contenuto del nuovo cybercrime disciplinato dall'art. 612-ter c.p.' (2020) Rivista di Diritto Penale Contemporaneo, p.7-9. Access online:

or his genitalia or the reproduction of his sexual acts, he certainly could not complain about the violation of a kind of freedom he or she has instead already exercised because he knowingly decided to renounce to the confidentiality that the legal system had insured.[142]

Nonetheless, if the consent lacks and sexually explicit contents are spread to other people, there is the presence of a serious interference in the depicted person's private and sexual life, that maintains his own negative impact to sexual privacy, regardless the motivation that determined the dissemination.[143]

The reproduction of body parts or acts relating to a particularly protected intimate sphere of the person has been illegally stolen or, in any case, arbitrarily exposed to the public and this annul the dominion of the depicted person over her intimacy.[144] Therefore, the arbitrariness of the reproduction and of the dissemination explains the harms for the depicted person and justifies the criminal answer from the legal system.[145]

In line with Amore's vision, Romano underlines that somebody's privacy in his or her sexually explicit footage should not conclude upon disseminating those pictures or videos with a partner, because the use of that information has been granted only in the context of the intimate relationship. To broadly spread the images means to utilize private and intimate information concerning sexual life for a purpose other than that granted and, thus, represent an invasion of sexual privacy punishable with imprisonment and monetary fine stated by article 612 ter of the Italian Criminal Code.[146] Thus, it seems likely that this provision applies to the reproduction and spread of sexually explicit deepfakes.

3.3 Virtual child pornography

When a minor is depicted in a sexually explicit deepfake footage, article 600 quater.1 of the Italian Criminal Code, which defines virtual child pornography, is applicable. This article represents another response of the Italian Criminal law systems against the invasion of sexual privacy.

Virtual child pornography has been criminalized in Italy since 2006. Indeed, the law n. 38 of 6 February 2006 named "Provisions for fighting sexual exploitation of children and child pornography, including via Internet" modified the Italian Criminal Code and added to its provisions the article 600 quater.1, named "Virtual pornography".

This article states that "the provisions of Articles 600-ter and 600-quater (which notably criminalize child pornography and the possession of pornographic material) shall be applied even when pornographic material shows virtual images produced by using images of minors (i.e. under the age of 18) or part of them, however the penalty is decreased by one third. Virtual images shall mean images produced through techniques of graphic processing that are not completely associated with real situations, whose quality of depiction makes unreal situations seem to be real".

Thus, Italian criminal law makes a distinction between production and sale of virtual child pornography material (punished with imprisonment for four to nine years and fine for 17.000 to

https://www.researchgate.net/publication/338833887_La_tutela_penale_della_riservatezza_sessuale_nella_societa_digitale_Contesto_e_contenuto_del_nuovo_cybercrime_disciplinato_dall'art_612-ter_cp.

[142] *Id.*

[143] *Id.*

[144] *Id.*

[145] *Id.*

[146] B. Romano, 'L'introduzione dell'articolo 612-ter del codice penale in materia di diffusione illecita di immagini o video sessualmente espliciti', (2020) Codice rosso. Commento alla l. 19 luglio 2019 n. 69, in materia di tutela delle vittime di violenza domestica e di genere, p. 105-112. Access online: <https://pure.unipa.it/it/publications/lintroduzione-dellarticolo-612-ter-del-codice-penale-in-materia-d.

174.000 euro), distribution, spread or advertisement (whose penalty is imprisonment for nine months to three and half years and fine for 1600 to 3400 euro) and offering and provisioning (punished with imprisonment up to two years and a fine for 1000 to 3400 euro).
Furthermore, the sole obtention or possession of virtual child pornographic material leads to penalty when the subjective element incurs. Indeed, whoever knowingly obtains or possesses pornographic material produced using persons under the age of eighteen is liable to imprisonment for a term up to two years and to a minimum fine of 1.000 euro.
In all the cases mentioned above the penalty is increased up to two thirds if the quantity of the materials is considerable.
The Italian Court of last Instance (Corte di Cassazione) dealt with the interpretation of Article 600 quater1 and the notion of virtual child pornography in its judgement n. 22265 of 13 January 2017, clarifying both its rationale and boundaries. Indeed, in this case an accused man had procured and held knowingly around 95.000 child pornography images through a sharing peer-to-peer system. Notably, they were drawings or comics representing minors practicing sexual intercourses that were defined by the first judge as "abject and gruesome"[147].
The Court stated it was not possible to exclude the existence of the criminal fact only because the pictures represented imaginary situations and minors that cannot be associated to real persons and that are "the pure result of graphic technology combined with author's sexual fantasy"[148]. Indeed, according to the judges, article 600 quater-1 does not only protect the sexual freedom and sexual privacy of a minor concretely represented and, therefore, identified, but rather preserve the intangibility of minors personality and the respect of time and way of development of his/her personality.[149] The legislator focuses, instead, on the contrast to those behavior that endanger minors' sexual intimacy and children are considered as a category needed of enhanced and equal protection[150]. Thus, all those behaviors, although not offensive toward an identified minor, that spread or increase the sexual attraction to children are punished because minors are not able to express a valid consent to sexual activity due to their psychological development and relational maturity.[151]
The provision against virtual child pornography is very useful when dealing with nonconsensual deepfake pornography, because the article explicitly mentions the virtual and computer-based dimension of this content. Sexually explicit deepfake pornography thus may fall within the scope of article 600 quater.1 of Italian Criminal Code. However, this can only be applied for footage depicting minors. It does not provide relevant legal remedy for people above the age of 18 who are portrayed in a deepfake because it protects the intangibility of minors' nature as such: it seems likely that this provision applies to the depiction of young-looking people represented as minors. However, there might not be chances for adults to find remedies under Italian virtual child pornography law.

3.4. Defamation and aggravated defamation

Defamation is broadly defined as a false "statement that tends to expose the individual to public contempt, ridicule, aversion, or disgrace, or induce an evil opinion of him in the minds of right-thinking persons, and to deprive him of their friendly intercourse in society".[152]

[147] Corte di Cassazione penale, section II, no. 22265 of 13/01/2017, paragraph 44.
[148] Corte di Cassazione penale, section II, no. 22265 of 13/01/2017, paragraph 137.
[149] Corte di Cassazione penale, section II, no. 22265 of 13/01/2017, paragraph 81.
[150] Corte di Cassazione penale, section II, no. 22265 of 13/01/2017, paragraph 90.
[151] Corte di Cassazione penale, section II, no. 22265 of 13/01/2017, paragraph 103.
[152] E. Meskys, A. Liaudanskas, J. Kalpokiene, P. Jurcys, *supra* note 40.

The Italian Court of last Instance has interpreted the notion of "statement" extensively: it comprehends images, writings or videos aimed at offending a person and suitable to harm the honor of a person.[153]

On a general level, some deepfakes are definitely not defamatory. Consider the example referenced above in which the former Italian prime minister, Mr. Matteo Renzi:[154] in this case, there is nothing shameful about such a video so as to invoke defamation because the character represented is fictitious and the representation is meant to be a caricature of the former prime minister.

However, outside of clear parodies, which do not give rise to defamation action, determining whether a footage is defamatory can be particularly difficult when edited videos are involved.[155]

In addition, in order for a defamation to be declared actionable, it is required a way of circulation that brings speech into the public territory where it can unreasonably disturb the constitutionally guaranteed free exchanges and circulation of ideas, such as the website communities: sexually explicit deepfakes are not constitutionally safeguarded because they are produced and disseminated to purposefully denigrate a public or private individual.[156]

Article 595 of the Italian Criminal Code outlines defamation as a damage to the reputation of a person through communication with several persons and there are three forms of aggravated defamation: through the allegation of a specific act; through the press or any other means of publicity, or through a public deed; and whether it is directed to a political, administrative or judicial body.[157] Thus, defamation is a criminal offence in Italy; penalties for defamation by means of the press or of any other mean of publicity, including televisions, online blogs and social networks represent aggravated forms of offence and may amount to imprisonment between six months and three years.[158]

However, both the Italian legal scholars and the Italian Courts have regularly confirmed that the exercise of the right to news reporting, the freedom of speech and the freedom of the press guaranteed in Article 21 of the Italian Constitution represents a cause of justification for the publication of defamatory footages and news, within the meaning of Article 51, paragraph 1 of the Criminal Code,[159] thus making the communication of information which harms the honor, the dignity or the reputation of another person non punishable.[160]

The Italian Court of last instance stated a landmark judgment[161] which continues to be persistently applied by Italian courts and specified the three criteria for the implementation of Article 51 of the Italian Criminal Code: first, the social function or social importance played by the information; then, the truth of the information, which may be presumed when the disseminator has seriously verified the sources of information.[162] To conclude, the Court set up the last criteria, the so called "restraint", referring to the edulcorated and civilized form of expression, which must not "violate the minimum dignity to which any human being is entitled".[163]

---

[153] Corte di Cassazione penale, section V, no. 8328 of 13/07/2015, paragraph 88.
[154] See Chapter I.
[155] *Id.*
[156] D. Harris, *supra* note 103.
[157] Opinion on the legislation on defamation of Italy adopted by the Venice commission at its 97th Plenary Session, European commission for democracy through law (Venice commission), 2013.
[158] *Id*.
[159] The article 51, paragraph 1 of Italian Criminal Cod states that exercise of a right or the fulfillment of a duty imposed by a law or by a legitimate order of a Public Authority excludes the criminal punishment.
[160] W. Bennett, S. Livingston, *supra* note 27.
[161] Corte di Cassazione civile, section I, no. 5259 of 18/10/1984.
[162] Corte di Cassazione civile, section I, no. 5259 of 18/10/1984, paragraph 97.
[163] Corte di Cassazione civile, section I, no. 5259 of 18/10/1984, paragraph 126.

When a perpetrator produces and disseminates sexually explicit deepfake videos, it seems likely that he or she defames the honor or good name of the depicted person and may be prosecuted on the basis of aggravated defamation. Indeed, the act of depicting someone while she or he is having a sexual intercourse is not a fact of social relevancy because it regards the intimate sexual sphere of the person. Furthermore, sexually explicit deepfake are fake footages, thus the second element of the truth of the information does not apply.
To conclude, disseminating pornographic footage without the consent of the depicted person is not a civilized form of expression and violates the dignity of the depicted person.
Thus, the three conditions stated by the Italian Court of last instance do not apply.
In addition, the Italian Court of last instance stated that the publication of pornographic images on a website for recipients different from those in relation to which the consent had previously given by the depicted person is defamation.[164]
Then, the Italian Court of last instance dealt with the following situation in its judgement 36076 in 2018:[165] an 18-year-old student created and spread online pornographic photomontage depicting two teachers. The Supreme Court stated that article 595 of Italian criminal Code applies when a photomontage is created in a context that implies a negative evaluation of the portrayed people.[166] Indeed, according to the Court, the offence to reputation occurs when the images, albeit fake, show intrinsically offence to the victims' reputation because they are portrayed in a scenario of obscenity and vulgarity.[167] Thus, there might be considerable chances that this provision applies also to sexually explicit deepfakes.
It is interesting to underline how the Italian Court of last instance equalizes social networks such as Facebook, Twitter and Instagram with a place open to the public. According to the Court, the social networks are thus considered like a square, even whether they are immaterial, due to the elevated number of accesses and visions they are able to guarantee.[168] Social networks are therefore public places where defamatory communication may regularly happen.[169]

3.5 Menace

Besides attacking the honor and the good name of the depicted persons, the sexually explicit footage can also be used as object of menace; indeed, the act of intimidating someone to produce an edited pornographic video or a sexually explicit deepfake depicting him/her is criminalized in Italy.
Menace is criminalized by article 612 of the Italian Criminal Code; on a general level, this crime consists of intimidation made through the prospect of unfair harm.[170] The Italian Criminal law places menace in the section of crimes against the individual freedom and punished it with a monetary fine up to 1032 euro.[171]
In particular, the Italian Criminal Code considers menace each conduct whereby an individual is intimidated with the prospect of unfair harm: the menace may be directed to a person or to his/her

[164] Corte di Cassazione penale, section III, no. 19659 of 19/01/2019, paragraph 119.
[165] Corte di Cassazione penale, section V, no. 36076 of 27/07/2018.
[166] Corte di Cassazione penale, section V, no. 36076 of 27/07/2018, paragraph 85
[167] Corte di Cassazione penale, section V, no. 36076 of 27/07/2018, paragraph 96
[168] Corte di Cassazione penale, section I, no. 37596 of 12/09/2014, paragraph 134.
[169] Corte di Cassazione penale, section I, no. 37596 of 12/09/2014, paragraph 138.
[170] G. Gatta, 'La minaccia. Contributo allo studio delle modalità della condotta penalmente rilevante' (2013), p.20-21. Access online: https://www.academia.edu/5445809/La_minaccia_Contributo_allo_studio_delle_modalit%C3%A0_della_condotta_penalmente_rilevante.
[171] *Id.*

assets and must be able to limit his/her physical or psychological freedom.[172] Beside unfair, the harm shall make the menaced person frightened and unstable.[173] However, each menace shall be properly assessed according to the circumstance, the condition of the agent and the effect on the victim.[174]
As Nesso underlines, the crime of menace is widely interpretated: it does not only identify the menace of unfair physical harm of the victims, but even the psychological harms;[175] the physical presence of the menacing person is not a necessary condition for the realization of the crime; it is, indeed, sufficient to prove the menacing agent's will to produce the real result of his/her intimidation.[176]
In addition, this crime does not arise only when intimidating acts are expressed orally: the most varied communication means, such as writings, gestures, text messages, e-mails, online messages can also be included in the menace.[177]
Thus, taken into consideration the broad interpretation of the article 612 of Italian Criminal Code made by the Courts and Italian legal scholars, when someone threatens to disseminate online a sexually explicit deepfake video depicting another person, the perpetrator may thus be prosecuted on the basis of this article. Indeed, the dissemination of the video causes undoubtedly unfair psychological and emotional distress for the depicted person, as analyzed in Chapter II.

3.6 Cyberbullying

The act of creating and disseminating sexually explicit deepfake that depicts a minor seems likely to be also a form of cyberbullying, which involves the use of information and communication technology to enforce aggressive behavior by an individual or group that aims at harming others.[178]
Indeed, cyberbullying seems to comprehend cases when cyberbullies send or publish on the internet altered images, such as photographs or videoclips of the victim, by modifying face or body of the target student in order to ridicule him or her or by making him or her the protagonist of sexually explicit scenes through the use of photomontages or deepfake technology.
The law of 29 May 2017, n. 71, named "Provisions for the protection of minors to prevent the phenomenon of cyberbullying" (“Cyberbullying Law”), represents the first attempt in Italy to regulate the phenomenon of cyberbullying through the law.
This law interestingly defines cyberbullying as "any form of pressure, aggression, harassment, blackmail, insult, denigration, defamation, identity theft, alteration, illicit acquisition, manipulation, illicit processing of personal data for the detriment of minors, carried out through electronic means".[179]
In addition, in order to guarantee the widest coverage of the phenomena, the definition of cyberbullying comprehends the dissemination of online content (also concerning one or more

[172] See Corte di Cassazione penale, section V no. 8193 of 14/01/2012, paragraph 88.
[173] See Corte di Cassazione penale, section V no. 17159 of 20/03/2019, paragraph 105.
[174] *Id.*
[175] F. Nesso, ‘La condotta tipica nel delitto di estorsione. Contributo alla teoria della violenza e della minaccia nel sistema penale’, Dirittifondamentali.it (February 2020). Access online:http://dirittifondamentali.it/wp-content/uploads/2020/06/Nesso-La-condotta-tipica-nel-delitto-di-estorsione.pdf.
[176] *Id.*
[177] See Corte di Cassazione penale, section V no. 35817 of 18/06/2018, paragraph 107.
[178] A. Sorrentino, A. Baldry, S. Cacace, ‘Cyberbullying in Italy’ (2018) International Perspectives on Cyberbullying, p. 231-249. Access online: https://link.springer.com/chapter/10.1007%2F978-3-319-73263-3_10.
[179] L. Musselli, ‘La legge 29 maggio 2017, n. 71 sul cyberbullismo: dal “limbo legale” ad una regolamentazione a carattere preventivo-amministrativo’ (2018) Privacy, Minori & Cyberbullismo. Access online: https://ebookcentral.proquest.com/lib/uvtilburg-ebooks/detail.action?docID=5434910.

components of the family of the minor involved) "whose intentional and predominant purpose is to isolate a minor or a group of minors by engaging in serious abuse, a harmful attack or ridicule".[180]
The main remedy that Cyberbullying Law provides in the case of acts of cyberbullying is the administrative procedure defined at article 2. This procedure, called "Notice and Takedown", is based on fast and procedural simplification in order to provide a prompt response to cyberbullying behavior.[181]
The legitimate persons who have the right to exercise the administrative procedure are minors over the age of 14 who have suffered an act of cyberbullying and their parents.[182] This represent a huge innovation: indeed, the active legitimation of the action is not only conferred to the parents, but it is also extended to minors from the age of 14 to the age of 17.[183]
The request shall be addressed to the data controller or the manager of the website or of the social media where the cyberbullying video is disseminated for the obscuring, removal or blocking of any other personal data of the minor, after preserving the original data.[184]
The procedure is then characterized by the provision of very close time scans in order to minimize the harm and offer prompt protection.[185] Whether within 24 hours following receipt of the request, the data controller or the website manager have not communicated that they have taken tasks for the requested obscuring, removal or blocking and whether, within 48 hours, they have not concretely done so or, in any case, when it is not possible to identify the data controller or the website manager, the claimant may send a similar request to the Italian Data Protection Authority who has the duty to proceed with the block measures within 48 hours from the receipt of the request.[186] Thus, the Notice and Takedown procedure establishes that the removal obligations are firstly imposed on the operators (e.g. the website and social network manager) and the Italian Data Protection Authority intervenes subsidiarily only in case of their non-compliance.[187]
The second main novelty introduced by the Cyberbullying Law is the institution of the warning of the Commissioner of the local Police provided in article 7.
The aim of the warning is to perform a dissuasive function, based on the authority of the subject who disposes it, towards the cyberbully, and to induce him to reflect and to desist from further harmful conduct.[188]
The warning procedure pursuant to article 7 of Cyberbullying Law consists of the summoning of the minor by the Commissioner of the local Police together with at least one parent or other person exercising parental control and responsibility and the effects of the warning ends when the minor cyberbully reaches the age of 18.[189]
What it is not clear from the Cyberbullying Law is whether the hypothetical presence of cyberbullying crime should be assessed during the warning procedure. In this regard, the jurisprudence of the highest Administrative Court (the "Consiglio di Stato") intervened on the matter and stated that "the

[180] *Id.*
[181] *Id.*
[182] *Id.*
[183] *Id.*
[184] *Id.*
[185] P. Pittaro, 'La legge sul cyberbullismo' (2017) Famiglia e diritto. Access online: https://arts.units.it/handle/11368/2907618#.X7o8zhNKhQI.
[186] *Id.*
[187] *Id.*
[188] *Id.*
[189] *Id.*

warning procedure performs a precautionary, preventive and educational function, and it is aimed at avoiding that the persecutory acts carried out against the bullied are repeated or at avoiding he cause of irreparable damages towards bullied minors".[190] Thus, "the full proof of the responsibility of the admonished minor is not required; however, it must be plausible that the cyberbullying conduct has been made together with the harm for the bullied minor".[191]

3.7 Cyberstalking

Cyberstalking is strictly linked with the crime of stalking. On one hand, stalking is defined as any "continuative harassing, threatening or persecuting behavior which: (1) causes a state of anxiety and fear in the victim(s), or; (2) ingenerates within the victim(s) a motivated fear for his/her own safety or for the safety of relatives, kin, or others associated with the victim him/herself by an affective relationship, or; (3), forces the victim(s) to change his/her living habits".[192]

On the other hand, Ziccardi defines cyberstalking as the conduct perpetrated through the use of the network: the stalker, through the network, shows various behaviors with the aim of harassing his victim directly or indirectly.[193] Computer and networks, indeed, offer to the cyberstalker different and broader modalities of action: the continuous sending of large quantities of e-mails and messages to the victim, spamming messages or e-mails with offensive and harmful content, the intrusion into the computer system of the victim through virus aimed at taking control of it (the so called "trojan horse") or damaging it, the online dissemination of information with harmful, offensive and sexually explicit content concerning the victim.[194]

Cyberstalking enters into the Italian criminal law context in 2013, as a result of the Law of 15th October 2013, n. 119 ("Cyberstalking Law"); indeed, the article 1 of the Cyberstalking Law modified the article 612 bis of the Italian Criminal Code and added a new paragraph that recognizes the new aggravated form of stalking committed through IT or telematic tools and states a higher criminal sanction punishable with imprisonment ranging from six months up to four years.[195]

The Italian Court of last instance had already recognized the existence of the phenomenon in 2010. Indeed, in its judgement n. 32404 on 16 July 2010, the Court dealt with the following situation: the perpetrator began to send his ex-fiancée via the social network Facebook sexually explicit numerous videos, pictures and messages that portrayed them at the moment of sexual intercourses.[196]

The Supreme Court specified that the sending such videos and messages constitutes the crime of stalking and found the existence of serious indications of guilt in the conduct of the man through the use of Facebook, which had provoked in the woman a state of profound discomfort and fear.[197] Furthermore, the judges underlined that the continuous portrayal of sexually explicit images depicting the victim during intimate moments with her ex-boyfriend had generated a constant state of anxiety in the woman because these images discredited her by representing her as a person thirsty for sexual

[190] Consiglio di Stato, section. III, no. 2599 of 25/05/2018, paragraph 121.
[191] Consiglio di Stato, section III, n. 2599 of 25/05/2018, paragraph 139.
[192] G. Ziccardi, 'Cyberstalking and electronic devices: relevant legal-informatics issues' (2012) 6 Italian Journal of Criminology. Access online: https://ojs.pensamultimedia.it/index.php/ric/article/view/516/499.
[193] *Id.*
[194] *Id.*
[195] Italian Criminal Code, article 612 bis, paragraph 2.
[196] Corte di Cassazione penale, section VI, no. 32404 of 16/07/2010, paragraph 92.
[197] Corte di Cassazione penale, section VI, no. 32404 of 16/07/2010, paragraph 118.

adventures and intercourses.[198] All these stalking conducts forced the woman to seek the care of a psychologist.[199]

In addition, in its judgement, n. 57764 in 2017, the Supreme Court affirmed the principle that messages and videos posted on social networks or online blogs integrate the objective element of the crime of stalking, specifying that the harmful attitude of such conduct does not only consist in any offence made through electronic means, but also in the dissemination of harmful data and content, regardless they are true or false which cause anxiety and suffering to the victim.[200]

3.8 Conclusion

The Italian Criminal Code offers several provisions aimed at protecting the legal interest of sexual privacy, psychological integrity and reputational sphere of the depicted people in sexually explicit deepfake images and videos.

First, the Italian legal system protects the individual's sexual privacy from illicit invasion through the criminalization of revenge porn in article 612 ter of the Criminal Code. Second, the intangibility of minors' personality and the respect of time and way of development of their personality, including their sexual development are the core legal interest at stake protected by article 600 quarter of Italian Criminal Code. Then, the crime of defamation stated at article 595 of Italian Criminal Code is a reaction against the exposure of the depicted individuals to public ridicule, aversion or disgrace and against the deprivation of their friendly intercourse in society. Thus, the legal interest protected by article 595 is the reputational sphere of individuals from third parties illicit intrusion and from its consequential damages. Furthermore, article 612 of the Italian Criminal Code criminalizes menace as the intimidation made through the prospect of unfair harm. The unfair harm is interpreted widely, thus the article, amongst the others, aims at protecting the harms in the victim's psyche derived from the action of the offender, such as the ones deriving from the online dissemination of sexually explicit deepfakes. In addition, the Cyberbullying law and, notably, the warning procedure stated at its article 7 contrasts the use of information and communication technology to enforce aggressive behavior by an individual or group that aims at inflicting physical, psychological and reputational harms to minors. Finally, the Cyberstalking law protects the psychological damages inflicted to the victim by the stalker through harmful data and content disseminated via IT and network devices, such as online blogs and social media, regardless the truth or falsity of their contents.

To sum up, the scope of these criminal frameworks often intersects with the act of creating and disseminating sexually explicit footage, and it may not be relevant whether this footage is real or a realistic depiction. For example, the Italian criminal law framework offers a broader protection in cases of virtual child pornography because all types of children depiction, including fictional and not linked to any real human portrayal, are illegal. This extensive shield for minors seems to be justified because of the assumption of their special vulnerability: article 600 quarter 1 of Italian Criminal Code defends the intangibility of minors' nature as such, the sexual attraction to children is punished because minors are not able to express a valid consent to sexual activity due to their psychological development and relational maturity. Thus, there might be only low chances for an extensive interpretation of this provision limited to young adults who may realistically be depicted as minors in sexually explicit deepfakes footages.

[198] Corte di Cassazione penale, section VI, no. 32404 of 16/07/2010, paragraph 99.
[199] Corte di Cassazione penale, section VI, no. 32404 of 16/07/2010, paragraph 100.
[200] Corte di Cassazione penale, section V, no. 57764 of 28/12/2017, paragraph 122.

Then, the legislator always intervenes *post factum*, after the commission of the crime, when the pornographic content has been already created and shared. The type of answer the legislator offers is sanctioning and it is based on the deterrent effect of imprisonment and pecuniary fines.

On one hand the sanctioning reaction from the Italian legislator shows undoubtful benefits.

First, criminal legislation may be more effective in deterring the dissemination of deepfakes. Indeed, a private plaintiff may often lack the economic resources needed to file a tort claim; but the state, which is the prosecutor in criminal cases, has the resources needed.[201] Furthermore, the imposition of criminal liability may deter potential disseminators of sexually explicit deepfakes due to the stigma and disgrace associated with a criminal conviction, in addition to the deterrent effect of the imprisonment itself.[202]

Second, criminal legislation may offer a different response to the depicted persons also from the retributive aspect, given the significant damage caused to victims and to the entire society.[203]

On the other hand, criminal deterrence may not be the only solution to offer a wide protection to the depicted person. A study conducted by Von Hirsch end other researchers focused on the connection between criminal law deterrence and imprisonment and showed that a weak link exists between increases in sentence severity up to imprisonment and the reduction of crime;[204] the risks of reiteration of the crime are still high, notwithstanding the penalty imposed by the legislator.[205]

[201] R. Rosenberg, H. Dancig-Rosenberg, 'Reconceptualizing revenge porn' (2020), 63 Arizona Law Review. Access online:https://poseidon01.ssrn.com/delivery.php?ID=363114095103071024071093087019091100127044006079024031064087070000111116071027085085099050107020030120050071065114118074121107058042000066077118070012093015113076107014011081121114092111113084118121017114010018023106000006004081096121075085121102111097&EXT=pdf.

[202] *Id.*

[203] *Id.*

[204] A. Von Hirsch, A. Bottoms, E. Burney, P. Wikström, 'Criminal Deterrence and Sentence Severity: An Analysis of Recent Research' (2009) 39(2) Alberta Law Review.

[205] *Id.*

Chapter IV: Data protection and right to image responses

4.1 Introduction

After the discussion on the application of Italian criminal law in chapter III, this chapter will analyze two more pieces of legislation offered by right to image and privacy and data protection law that increase and integrate the shield offered by the Italian law towards the depicted persons in sexually explicit deepfakes. The aim of this chapter is to discuss whether these legislative possibilities given by the Italian law protect the depicted persons from creation and dissemination of sexually explicit deepfakes and, if this is the case, to what extend they are able to offer a full restore to the depicted persons.

In addition, the chapter briefly debates whether data protection and right to image may be applied in practice when dealing with sexually explicit deepfakes. Paragraph 4.2 discusses whether, and if so, in what cases, deepfake footages can be considered personal data according to data protection law, then paragraph 4.3 specifically analyses the right to be forgotten. Paragraph 4.4 describe how Italian law discipline the right to image. Finally, paragraph 4.5 contains a short conclusion.

4.2 Deepfakes and personal data

The starting principle of every data protection law, including the General Data Protection Regulation (hereinafter the "GDPR"), is to protect the personal data of the natural persons, which are called data subjects in the European framework. Article 4, paragraph 1 of the GDPR defines the personal data as "any information relating to an identified or identifiable natural person".

Three elements are therefore necessary to identify a personal data: (i) information and (ii) an identifiable natural person, (iii) to which such information is related. Then, according to the GDPR:

"an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person".[206]

Thus article 4 of the GDPR does not clearly defines whether sexually explicit deepfake videos are personal data. In these videos, the depicted figures have the face and body of real persons and they act and use gestures in a way that real persons usually do in real life. However, face, physique, speech, acts or gestures do not belong to them, but they are artificial animations or graphics created by the developer.[207]Another type of pornographic deepfake videos occurs when the real face is superimposed on pornographic actors' bodies. In this case, the body is not artificially created, but belongs to a real person. In this second scenario, it is clear that body and face are the personal data of the real data subjects.[208]

On the other hand, lawyers discuss whether the artificial pornographic animation or graphics created by the developer and superimposed with the real face of the depicted person can be classified and interpreted as "personal data" according to the definition in the GDPR.

---

[206] GDPR, article 4, paragraph 1(1).

[207] B. Yildirim, C. Aydinli, 'Deepfake: An Assessment from The Perspective of Data Protection Rules', MONDAQ, (13th November 2019). Access online: https://www.mondaq.com/turkey/privacy-protection/863064/deepfake-an-assessment-from-the-perspective-of-data-protection-rules?.

[208] *Id.*

According to Yildirimin and Aydinli, “because of the fake nature of the content, consideration of data protection rules would be irrelevant because the content itself does not belong to a real individual”.[209]
On the other hand, it might be argued that the only use of the person's name or mimics without the data subject's consent might constitute an infringement and that a deepfake, even though fictional, counts as personal data under article 4 of the GDPR.[210]
Once discussed whether deepfake content may be considered as personal data, the concept of "personal data processing" is the basis in order to assess the legality of sexually explicit deepfakes within the scope of the data protection law.[211] Indeed, the GDPR states an extensive interpretation of the concept of data processing. According to the GDPR "'processing means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction".[212]
The fake pornographic content is usually created by combining and merging real pictures, videos and voices of the depicted persons, all of which are considered as personal data. Therefore, there are not rooms for uncertainty that personal data of the victim can be processed at least while the fake footage is being created.[213]
In addition, article 2 of the GDPR delimitates the material scope of the European data protection law and states the types of personal data processing which are outside the scope of the Regulation. First, the GDPR does not apply to the processing of personal data for household functions, which means personal data processed in the course of a purely personal or household activity, without connection to any professional business or that are not spread to more people than closest friend or family’s members.[214]
Second, the processing of personal data by competent authorities for law enforcement purposes is outside the GDPR’s scope: this happens when the Police is investigating about a crime.[215]
Third, according to article 2, personal data processed for the purposes of safeguarding national security or defense is outside the GDPR’s scope.[216]
The only exemption according to article 2 that seems relevant and can be connected and applied to certain types of sexually explicit deepfakes is the household exemption. Indeed, when the creator of the deepfake produces the pornographic content for his or her own enjoyment, without online dissemination, the perpetrator is not subject to the GDPR.

4.3 The right to be forgotten

In light of the above paragraph, whether sexually explicit deepfakes are considered as information related to an identifiable natural person, then this fake footage is protected within the scope of the GDPR. Such protection grants the depicted data subject the right to request the erasure of the fake

[209] *Id.*
[210] See N. Schmidt, ‘Privacy law and resolving deepfakes online’, IAPP blog, (30th January 2019). Access online: https://iapp.org/news/a/privacy-law-and-resolving-deepfakes-online/.
[211] *Id.*
[212] *Id.*
[213] *Id.*
[214] GDPR, article 2, paragraph 2(c).
[215] GDPR, article 2, paragraph 2(d).
[216] GDPR, article 2, paragraph 2(d).

footage together with monetary compensation, if any damage is suffered as consequence of the unlawful processing of personal data.[217]

Indeed, the GDPR represents the cornerstone of the current Italian legislation on data protection and contains the first legislative embodiment of the right to be forgotten.[218]

The right to be forgotten has a jurisprudential origin in Google Spain case,[219] where the Court of Justice of the European Union held that an Internet search engine operator shall take into consideration requests from individuals to eliminate links to freely accessible web pages that result from the search on their name.[220]

Thus, when information relating to an individual is not adequate, relevant, proportionated, data subjects have the right to request erasure of their personal data, according to article 17 of the GDPR. The right to be forgotten does not have an absolute nature, but shall be balanced with other rights and interests, such as the right to information and freedom of expression.

Since sexually explicit deepfake can be considered as personal data when they are massively published online on several social media and blogs because the household exemption stated in article 2 of the GDPR does not apply, the portrayed person could request erasure of these sexual footages under article 17 of the GDPR to internet service providers, such as search engines or social networks. Notably, sexually explicit deepfakes disseminated online are examples of unlawful processing of personal data according to article 17(1)(d) GDPR. Data processing is only lawful when one of the bases declared in article 6 GDPR applies, but when non-consensual deepfake pornography is posted online by somebody who is not the person portrayed in the footage, and this represents the common scenario, none of the bases of article 6 GDPR seem to apply.[221]

Furthermore, the right to privacy of the data subject who requests the erasure of the video also needs to be balanced with other rights of interested third parties and the freedom of expression. Indeed, the relationship between the protection of personal data and freedom of expression is regulated by Article 85 of the GDPR. According to this article, "Member States shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression".[222] The fact that the dissemination of sexually explicit contents against the will of the depicted persons may happen for academic or literary reasons is absolutely off-chance and thus none of the balances stated in article 85 seems to apply.

In addition, because there is no Italian case law regarding specifically the interaction between the GDPR and deepfakes, the same assumptions on defamation stated at 3.4 can be made. In sexually explicit deepfakes it seems clear that the right to privacy of the depicted person prevails over the rights to information and freedom of expression. The controller has thus the duty to erase personal data without undue delay when the right to erasure applies and in, certain cases, he also has to inform other controllers who process the personal data that deepfake footage should be erased.[223]

---

[217] GDPR, article 17.

[218] F. Di Ciommo, 'Privacy in Europe After Regulation (EU) No 2016/679: What Will Remain of the Right to Be Forgotten?' (2017) Italian Law Journal. Access online: http://theitalianlawjournal.it/data/uploads/3-italj-2-2017/pdf-singoli/623-di-ciommo.pdf.

[219] ECJ 13 May 2014, ECLI:EU:C:2014:317 (Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González).

[220] F. Di Ciommo, *supra* note 218.

[221] *Id.*

[222] GDPR, article 85, paragraph 1.

[223] GDPR, article 17, paragraph 2.

To sum up, the depicted persons are legitimated to exercise the right to erasure in order to eliminate sexually explicit deepfake videos from the Internet. However, the erasure of the video may happen only after the request of the data subjects to the controller who is processing the data and, when the video is already disseminated online on several webpages, the portrayed person shall forward the request to different controllers. This may lead to three main practical difficulties: first, it may happen that the depicted person becomes aware of the pornographic video depicting her or him after a long time, sometimes after several months, and, during that period, deepfakes remain to circulate online. Second, even after the target of the video by the depicted person, lot of time and effort is demanded because the request shall be addressed to different service providers, which are supposed to promptly reply and delete the deepfake. The third problem is that, even after the targeting and erasure of the video online, downloaded deepfakes on personal devices are still present and they are likely to continue to be spread via other channels, such as the dark web. For example, it is reported some Telegram chat groups continued to contain pornographic deepfake footage even after the complaint of the depicted Italian persons.[224]

Beside the practical problems, another limit of data protection law is its focus on the controller, such as social networks, online search engines and users, who does not necessarily coincide with the perpetrator.

Indeed, according to article 4 of the GDPR the data controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.[225]

Once a content has been posted on social networks, the purpose of this dissemination is to make it viral and let all the users to see and share it. Thus, it seems that social networks and search engines are data controllers together with all the users that have posted that specific content online. Therefore, once deepfake videos have gone viral or simply disseminated through several platforms by numerous users, it becomes really complicated to prosecute and fine under the GDPR the original perpetrator and he remain unconscious of the consequences that his conduct has caused to the victims.

For all the reasons mentioned above, the application of the right to be forgotten may not be the principal choice for the depicted persons to stop the online spread of sexually explicit deepfake videos.

A fortiori, it is emblematic that the recommendations of Italian Data Protection Authority Guidelines on deepfake published in December 2020 mainly focus on what the users can do to defend themselves from risks caused by deepfakes rather than on the safeguards of data protection law. Notably, according to these Guidelines, "the data protection authorities can intervene to prevent and sanction violations of data protection law; however, the main and most effective defense tool is always given by the responsibility and the attention of users."[226] The Italian Data Protection recommendations are to avoid uncontrolled dissemination of personal images and to remember that images posted on social medias are likely to remain online forever and that any user can download them.[227]

---

[224] See R. Rijitano, 'Deepfake su Telegram, c'è un bot che spoglia le donne: quasi 700 mila vittime', Repubblica, (20th October 2020). Access online: https://www.repubblica.it/tecnologia/sicurezza/2020/10/20/news/deepfake_un_bot_sveste_le_donne_oltre_100mila_vittime-271131375/.

[225] GDPR, article 4, paragraph 1(7).

[226] Autorità Garante per la Protezione dei dati personali (Italian Data Protection Authority), 'Deepfake. Il falso che ti ruba la faccia (e la privacy)', (December 2020). Access online: https://www.garanteprivacy.it/documents/10160/0/Deepfake+-+Vademecum.pdf/478612c7-475b-2719-417f-869e5e66604e?version=2.0.

[227] *Id.*

The second recommendation is to learn how to recognize a deepfake. Notwithstanding it may be often difficult to notice, there are elements that may help to distinguish a real video from a deepfake: the image may appear pixelated, grainy, or blurry, depicted persons' eyes can sometimes move unnaturally, mouth may appear deformed or too large when the person is talking, the light and shadows on the face may appear abnormal.[228]
Then, it is it is absolutely necessary to avoid sharing a video without the consent of the depicted person, whether there is the minimum doubt about the reality of the footage. It is also recommended to report it as a possible fake to the platform that hosts it, for example, a social media.[229]
Finally, when the user believes that the deepfake was used in a way that committed a crime or a privacy violation, he or she shall contact the police or the Italian data Protection Authority.[230]

4.4 The right to image and deepfakes

Article 96 of Law 633/1941 (hereinafter the "Italian Copyright Law") states that the portrait of a person cannot be showed, reproduced or commercialized without his or her consent, unless the reproduction of the is justified by the reputation or public office carried on, from the need of justice or police, from scientific, educational or cultural purposes, when reproduction is linked to facts, events, public interest ceremonies or held in public.
In any case, according to article 97, second paragraph, the picture or video shall not be shown or commercialized when the display or trade causes prejudicial to the honor, reputation or dignity of depicted person.
In addition to the provisions of Italian Copyright law, article 10 of the Italian Civil Code states that whether the image of a person or its parents, spouse or children has been exposed or published illicitly, or whether the publication has damaged the dignity or reputation of the portrayed persons, the Judicial Authority may order the end of the abuse and compensatory damages to the victims.
The portrait right is linked to the right to protection of personal life in article 8 of the European Convention of Human Rights (hereinafter the "ECHR"). Indeed, the landmark judgement of the European Court of Human Rights in Reklos and Davourlis v. Greece states that the notion of private life in article 8 ECHR shall be interpreted broadly, and it covers the right to identity and the right to personal development.[231] With regard to a person's image, the Court states that it constitutes one of the principal traits of his or her personality because it reveals the person's unique characteristics and distinguishes the person from his or her peers.[232] Therefore, the protection of image is fundamental for personal identity and development and the Court concludes that everyone shall have the right to control the use of his or her image.[233]
Even the Italian jurisprudence elaborated on the abuses of the right to image and offered an extensive interpretation of the abuses of the right to image.
First, with regard to the consent, the Italian Court of last Instance, affirmed that the consent for the publication of images required by the law must be explicitly given, though not necessarily in writing form and it may be limited and restricted to some uses.[234]

[228] *Id.*
[229] *Id.*
[230] *Id.*
[231] ECHR 15 January 2009, case 1234/05 (Reklos and Davourlis v. Greece), paragraph 39.
[232] ECHR 15 January 2009, case 1234/05 (Reklos and Davourlis v. Greece), paragraph 40.
[233] ECHR 15 January 2009, case 1234/05 (Reklos and Davourlis v. Greece), paragraph 40.
[234] Corte di cassazione civile, section III, no. 10957 of 06 May 2010, paragraph 63.

Furthermore, the Court of Appeal of Campobasso precised that the reproduction of images without the depicted person's consent is lawful only whether it is necessary for public information, and therefore in all the other cases, including sexually explicit deepfakes, the unauthorized reproduction and dissemination of images lead to both pecuniary and non-pecuniary compensation to the depicted persons.[235]

In addition, the Tribunal of Pordenone stated that the unauthorized publication of an image, used for advertising purposes, entails compensation for pecuniary and non-pecuniary damages in favor of the depicted persons, regardless of the denigratory content of the picture; the compensation is therefore due to the sole fact of the lack of consent to publication.[236]

In line with this sentence the judicial decree no. 5359 of 7th November 2019 issued by the Tribunal of Bari specified that the conduct of publishing the face of somebody online without his or her previous consent is sufficient to integrate the abuse of the right to image of the portrayed person.[237] The damaged party has the right to obtain the cessation of this abusive conduct and, therefore, the deletion of photos and videos from social networks.[238] The Court underlined that the face of the person posted on social network shall appear and be recognized clearly, regardless the background and all the other elements of the footage.[239] The amount of compensation may vary on the basis of different criteria, such as case-by-case circumstances, the damage suffered and the time of the online publication.[240]

The right to image could be implemented to offer protection for the depicted persons in sexually explicit deepfakes, but it brings forward several problems. First, the victim itself shall act and bring the case to court. This may require efforts in terms of financial costs, time consuming and emotional distress and may make the victim diffident to carry an extra burden: indeed, the victim needs to get in contact with the perpetrator who first starts to disseminate the sexually explicit footage and he or she shall search the pornographic deepfakes online. In contrast, when the depicted persons sue a perpetrator under criminal law, a public prosecutor begins the process once there is adequate evidence, which lead a minor level of pressure on the victims, because they do not have to take these steps alone.

Another problem is that it might be complicated for the depicted person to detect the perpetrator once the video has been leaked online because the perpetrator can effortlessly remain anonymous, and without the identity of the creators or spreaders of sexually explicit deepfake videos, the efforts in order to take legal remedies against them remain unproductive. On the other hand, the public prosecutor and the judicial police have more powers and possibilities to discover their identity and thus it might be more efficient to report the case at the police and sue under criminal law instead of taking steps through data protection and copyright law.

Furthermore, it is fundamental to underline the global nature of the Internet, which allows access to worldwide information and the creation of a worldwide sharing of pictures and videos, including sexually explicit deepfakes videos. As Maier underlined, "due to the global and borderless nature of the Internet, legislation (including the Italian criminal law, copyright law and privacy and data protection law) tries to somehow address the fact that many of the actions and effects within the

[235] Corte d'appello di Campobasso, section Civile, sentenza no. 84 of 21 February 2019.
[236] Tribunale di Pordenone, section Civile, sentenza no. 634 of 29 August 2017.
[237] Tribunale di Bari, section I Civile, ordinanza no. 5359 of 7 November 2019, paragraph 45.
[238] Tribunale di Bari, section I Civile, ordinanza no. 5359 of 7 November 2019, paragraph 47.
[239] Tribunale di Bari, section I Civile, ordinanza no. 5359 of 7 November 2019, paragraph 48.
[240] Tribunale di Bari, section I Civile, ordinanza no. 5359 of 7 November 2019, paragraph 50.

territory do not actually have physically taken place there".[241] This inevitably leads to slowly paced remedies which are limited to territorial jurisdiction of legislation and courts: "the problem here is that the approach ignores the fact that in cyberspace, certain acts have effects all over the world, regardless of the location of the perpetrator".[242] The consequence of tribunals exercising authority over online actions on the basis of their potential accessibility within a sovereign territory is problematic because it basically necessitates Internet providers and users to be compliant with all the substantive legislation in the world in order to completely avoid responsibility and an international system of legal and judicial reciprocity should be established, that is, according Maier's view, unworkable in practice.[243]

4.5 Conclusion

Data protection law and right to image represent two effective options to increase the protection and the legal remedies offered to depicted persons in sexually explicit deepfakes. Both data protection and right to image are interconnected and it is not a case that the GDPR has also itself evolved from the right to private life stated in article 8 ECHR. This chapter looks towards human right to private life, dividing it into two parts: protection of personal data and protection of personal identity, both to ensure adequate protection of private life and personal development.

On one hand, the GDPR, amongst the other provisions, allows the erasure request of the videos distributed online to data controllers; on the other, the Italian Civil Code and its jurisprudential interpretation and the right to private life under the ECHR imposed pecuniary compensation to perpetrators for the unauthorized publication of pictures and images portraying a physical person.

However, although these two pieces of legislation helps to integrate the protection offered by the Italian criminal law, they are not sufficient to fully hinder the creation and dissemination of sexually explicit deepfakes video. Indeed, data protection law and right to image implementation always react after the creation and dissemination of the footage made by the perpetrator; videos may still be downloaded, shared, found online in the future and may produce additional damage to the victim.

In addition, the right to image can intervene in cases of non-consensual deepfake videos, but it may be more preferable to sue the perpetrator under Italian criminal law because this gives less burden and pressure on the depicted persons and offer the opportunity to utilizes more resources and tools in order to gather evidence, notably through the powers that the judicial police have.

Furthermore, legal and territorial responses, including data protection and right to image, remain inevitably limited and incomplete because of the borderless nature of the internet.

Legislation alone is thus not sufficient to stop sexually explicit deepfakes from determining harm for the depicted persons: at this stage, the actions that the users can preventively do to defend themselves from risks caused by deepfakes rather than the legal safeguards and responses seems more realistic, practical and efficient.

---

[241] B. Maier, 'How has the law attempted to tackle the borderless nature of the Internet?', (2010), 18International Journal of Law and Information Technology, 2. Access online: https://sso.uvt.nl/login?rid=ir82szLnSkVuNbayQ3OcsikF__Km6AT6knjSptuYTw8ABbfDyFhcuUdVWWxlldWjObDCB6xAJc5sAHNpbXBsZXNhbWxwaHAAaHR0cHM6Ly9zYW1sLnV2dC5ubC9tb2R1bGUucGhwL2FzZWxlY3QvY3JlZGVudGlhbHMucGhwP3NzcF9zdGF0ZT1fNWQ0MzMyMjJiNGE1OGM4MjZlMDA5OGFlYzUzNGRkZDIxM2I1NTczNmEyJTNBaHR0cHMlM0ElMkYlMkZzYW1sLnV2dC5ubCUyRnNhbWwyJTJGaWRwJTJGU1NPU2Vydmljes5waHAlM0ZzcGVudGl0eWlkJTNEaHR0cHMlMjUzQSUyNTJGJTI1MkZlbmdpbmUuc3VyZmNvbmV4dC5ubCUyNTJGYXV0aGVudGljYXRpb24lMjUyRnNwJTI1MkZtZXRhZGF0YSUyNmNvb2tpZVRpbWUlM0QxNjA5NDI2Mzkx&a-select-server=sso.uvt.nl.

[242] *Id.*

[243] *Id.*

Chapter V: Conclusion

5.1 Main research question

Although the phenomenon of sexually explicit deepfakes has been dramatically spreading all over Europe and in Italy, currently there is no academic Italian literature on the relationship between sexually explicit deepfakes and legal responses against them: legal academic literature directly dealing with sexually explicit deepfake videos in Italy is almost entirely absent and, in this regard, this thesis plays a pioneering role.

This is a gap in the literature, which the research of this thesis aimed to fill.

It is fundamental to research this specific type of deepfakes for two main reasons. First, because non-consensual pornography is the typology of deepfakes most disseminated online, and it continues to gain popularity. The second reason is that, at the moment, there is a legal vacuum in both Italian and European Union law. The legislation is thus considered deficient because it is regularly uncertain whether sexually explicit deepfakes fall within the scope of the legislation. The explication of this uncertainty is found because the law does not explicitly mention deepfakes, and there is also no case law yet that directly elucidates the criminal and civil law responses to protect and restore the depicted persons in sexually explicit deepfakes. The answer to whether it is against the law to produce and disseminate false pornography on the internet is complicated.

In order to fill the gap that is created because of the absence of Italian legal literature concerning sexually explicit deepfakes and in order to offer a starting point for additional research, the thesis answers to the following research question:

To what extent does the current Italian criminal law framework, the GDPR and the right to image in the Italian context protect individuals depicted in sexually explicit deepfakes?

5.2 Findings

The research showed that several harms for the depicted persons which are reported in the context of revenge porn, may still be present even if the content is a deepfake. The harms are classified in harms deriving from invasion of sexual privacy, psychological and emotional distress and reputational damages.

Once clarified the harms caused by the dissemination of sexually explicit deepfakes, the thesis put the attention on criminal law responses to the dissemination of sexually explicit deepfake and shows that different Italian criminal provisions may be applicable in cases of nonconsensual deepfake pornography. Notably, they are Revenge pornography, Virtual child pornography, Defamation and aggravated defamation, Menace, Cyberbullying and Cyberstalking.

There are no explicit case laws regarding the application of revenge pornography law to the dissemination of sexually explicit deepfake. However, it is reasonable through doctrinal interpretation that depicted person may invoke article 612 ter of Italian Criminal Code. On the other hand, case laws have already defined the scope of virtual child pornography and article 600 quarter I of Italian Criminal Code which includes sexually explicit deepfakes.

In addition, the Italian Court of last Instance found that the offence to reputation necessary for in cases of defamation occurs when the images, albeit fake, show intrinsically offence to the victims' reputation because they are portrayed in a scenario of obscenity and vulgarity. This implicitly means that nonconsensual deepfake pornography fall within the scope of article 595 of the Italian Criminal Code. In line with this extensive view and taken into consideration the broad interpretation of menace made by the Courts and Italian legal scholars, when someone threatens to disseminate online a

sexually explicit deepfake video depicting another person, the perpetrator may thus be prosecuted on the basis of the article 612 of Italian Criminal Code.
Then, with regards to cyberbullying, albeit there is no explicit cases law which may illuminate the context, it seems clear that the scope of Cyberbullying law to comprehends cases when cyberbullies send or publish on the internet altered images, such as photographs or videoclips of the victim, including sexually explicit deepfakes.
Finally, the Italian Supreme Court specified that the harmful attitude of the crime of cyberstalking does not only consist in any offence made through electronic means, but also in the dissemination of harmful data and content, regardless they are true or false, which cause anxiety and suffering to the victim and it is reasonable to affirm that sexually explicit deepfakes fall within the scope of article 612 bis of the Italian Criminal Code.
All these provisions protect the legal interest menaced by the dissemination of sexually explicit deepfakes. The legal interest protected by revenge pornography and virtual child pornography is sexual privacy; defamation and menace protect the legal interest of phycological sphere. Finally, cyberbullying and cyberstalking law protects both psychological and reputational field.
In addition, the thesis found that the right to be forgotten from the GDPR and the right to image may be applicable in cases of sexually explicit deepfakes. They both represent two effective options to increase the protection and the legal remedies offered to depicted persons in sexually explicit deepfakes. Notably, the GDPR allows the erasure request of the videos distributed online to data controllers and the Italian Civil Code and its jurisprudential interpretation together with the right to private life under the ECHR imposed pecuniary compensation to perpetrators for the unauthorized publication of pictures and images portraying a physical person. The protection offered by the GDPR takes place when the data subjects' rights are exercised by the depicted persons towards data controllers and internet search engines.

5.3 Implications

The research shows that different Italian provisions seem to apply in cases of sexually explicit deepfake videos. However, at the moment there is no governmental clarification and the current provisions would need to be amended in order for sexually explicit deepfakes to fall within their scope more evidently, without extensive interpretation.
Furthermore, the research finds strengths and weaknesses of the criminal law approach towards sexually explicit deepfakes: the type of answer the legislator offers is sanctioning and it is based on the deterrent effect of imprisonment and pecuniary fines.
In addition, the Italian legislator applies a supplementary protection in cases of sexually explicit deepfakes depicting minors because all types of children pornographic depiction, including fictional and not linked to any real human portrayal, are illegal.
According to the author's point of view, the aim of protecting children nature as such is absolutely shareable and finds a reason because of the uniqueness of children's status due to their psychological development and relational maturity, which deserve broader protection. Thus, this shield shall remain limited to children and youngsters under the age of 18.
Then, the research underlines that data protection law and the right to image represents valid options for the depicted persons, by offering substantial pecuniary remediation for suffered damages.
Finally, it is clear that in all the mentioned cases the legislator intervenes *post factum*, when the pornographic content has been already created and shared and this may be too late.

Thus, the Italian legislator would need to cooperate with other stakeholders such as technology developers and social networks in order to stop "by design" the dissemination of pornographic deepfakes and make not possible to spread them. The sole legislation is not enough, thus cooperation with other actors is the only solution to establish an efficient plan against the harms generated by these types of deepfake videos.

To sum up, this thesis finds three main limitations. First, the lack of legal certainty in the Italian scenario forces jurisprudence and scholars to and extensive interpretation when dealing with cases of sexually explicit deepfakes. This interpretation is not always clear and may generate confusion. Second, the nature of post factum legal responses does not encourage the prevention of the creation and dissemination of sexually explicit deepfakes online. Third, the lack of international cooperation between States and social media platforms limits the implementation of preventive protection for the depicted persons in sexually explicit deepfakes.

5.4 Final thoughts

"I felt so embarrassed. I was sent to the hospital with heart palpitations and anxiety, the doctor gave medicine to me. But I was vomiting, my blood pressure shot up, my body had reacted so violently to the stress".[244] These words are reported from an interview given by Rana Ayyub, an Indian journalist victim of pornographic deepfake that left her devastated. This attack was organized after she campaigned and claimed justice for a rape and murder episode happened in the Indian city of Kathua in 2018. Some local leaders had supported the accused persons claiming they were incriminated unjustifiably because they were Hindu. When Rana expressed her position, she faced online hate on Twitter.

It is fundamental to realize that becoming the "star" of sexually explicit deepfakes may potentially happen to everyone because nowadays it is absolutely common to upload innocuous digital pictures online through social media platforms: the phenomenon will inevitably grow in the future and it has no boundaries.

The matter deserves more attention and globally coordinated answers from legislators and societies in order to stop the dissemination of these harmful types of content.

Prevention is the key term to avoid that those reported words will be repeated again together with the tragic stories of the victims.

[244] R. Chatterjee, *supra note* 38.

Bibliography

Articles

N. Amore, 'La tutela penale della riservatezza sessuale nella società digitale. Contesto e contenuto del nuovo cybercrime disciplinato dall'art. 612-ter c.p.' (2020) Rivista di Diritto Penale Contemporaneo. Access online: https://www.researchgate.net/publication/338833887_La_tutela_penale_della_riservatezza_sessuale_nella_societa_digitale_Contesto_e_contenuto_del_nuovo_cybercrime_disciplinato_dall'art_612-ter_cp.

R. Behun, E. Owens, 'Youth and Internet Pornography: The impact and influence on adolescent development'. 2019.

W. Bennett, S. Livingston, 'The disinformation order: Disruptive communication and the decline of democratic institutions', (2018), 33 European Journal of Communication.

A. Bridges, R. Wosnitzer, E. Scharrer, C. Sun, R. Liberman, 'Aggression and Sexual Behavior in Best-Selling Pornography Videos: A Content Analysis Update" (2010), 16(10) Violence against women.

G. M. Caletti, 'Il testo del disegno di legge "Codice Rosso" (Text on the "Codice Rosso" legislatve bill)' (2019) Diritto Penale Contemporaneo. Access online: https://archiviodpc.dirittopenaleuomo.org/d/6622-il-testo-del-disegno-di-legge-codice-rosso-revenge-porn-costrizione-o-induzione-al-matrimonio-defor.

G. M. Caletti, 'Sexual Freedom and Privacy in the Age of Internet. Article 612-ter of the Italian Criminal Code and Criminalization of Non-consensual Pornography' (2019) Rivista Italiana di diritto e procedura penale. Access online:https://www.academia.edu/43533049/LIBERT%C3%80_E_RISERVATEZZA_SESSUALE_ALL_EPOCA_DI_INTERNET_L_ART_612_TER_C_P_E_L_INCRIMINAZIONE_DELLA_PORNOGRAFIA_NON_CONSENSUALE_Sexual_Freedom_and_Privacy_in_the_Age_of_Internet_Article_612_ter_of_the_Italian_Criminal_Code_and_Criminalisation_of_Non_consensual_Pornography>.

Chesney B., Citron D., 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security', (2019) 107 California Law Review. Access online: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3213954

D. Citron, 'Criminalizing Revenge Porn', Wake Forest Law Review, Vol. 49, 2014. Access online:https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2368946.

D. Citron, 'Sexual Privacy' (2019) Yale Law Journal.

F. Colleti 'Revenge porn: the concept and practice of combatting nonconsensual sexual images in Europe' (2017) European Master's Degree in Human Rights and Democratization - University of Latvia.

S. Dack, 'Deep fakes, fake news and what comes next', (2019) Henry M. Jackson School of International Studies - University of Washington. Access online: https://jsis.washington.edu/news/deep-fakes-fake-news-and-what-comes-next/#_ftn8.

R. Delfino 'Pornographic deepfakes: the case for federal criminalization of revenge porn's next tragic act' (2019) Fordham Law Review 887. Access online: https://ir.lawnet.fordham.edu/flr/vol88/iss3/2.

R. Delfino, 'Pornographic Deepfakes – Revenge Porn's Next Tragic Act – The Case for Federal Criminalization' (2019) 88 Fordham Law Review. Access online: https://ir.lawnet.fordham.edu/flr/vol88/iss3/2.

F. Di Ciommo, 'Privacy in Europe After Regulation (EU) No 2016/679: What Will Remain of the Right to Be Forgotten?' (2017) Italian Law Journal. Access online: http://theitalianlawjournal.it/data/uploads/3-italj-2-2017/pdf-singoli/623-di-ciommo.pdf.

A. Dodge, E. Johnstone E., 'Using Fake Video Technology to Perpetrate Intimate Partner Abuse', (2019). Access online: https://www.cpedv.org/sites/main/files/webform/deepfake_domestic_violence_advisory.pdf.

M. Eneman, A. Gillespie, B. Stahl, 'Criminalizing fantasies: the regulation of virtual child pornography', (2009), Proceedings of the 17th European conference on information systems. Access online: https://www.researchgate.net/profile/Bernd_Stahl/publication/265357703_CRIMINALISING_FANTASIES_THE_REGULATION_OF_VIRTUAL_CHILD_PORNOGRAPHY/links/543186210cf277d58e982ac8/CRIMINALISING-FANTASIES-THE-REGULATION-OF-VIRTUAL-CHILD-PORNOGRAPHY.pdf.

M. Fertik, 'Your Future Employer Is Watching You Online. You Should Be, Too' (2012) Harvard Business Review. Access online: https://hbr.org/2012/04/your-future-employer-is-watchi.

L. Floridi, 'Artificial Intelligence, Deepfakes and a Future of Ectypes' (2018) Philosophy & Technology 31. Access online: https://link.springer.com/article/10.1007/s13347-018-0325-3.

A. Flynn, N. Henry, 'Image-Based Sexual Abuse: An Australian Reflection in Women & Criminal Justice', (2019). Access online: https://www-tandfonline-com.tilburguniversity.idm.oclc.org/doi/full/10.1080/08974454.2019.1646190.

K. Gabriel, 'Feminist revenge: seeking justice for victims of nonconsensual pornography through revenge porn reform' (2019), 44 Vermont Law Review. Access online: https://lawreview.vermontlaw.edu/wp-content/uploads/2020/07/06-Gabriel.pdf.

G. Gatta, 'La minaccia. Contributo allo studio delle modalità della condotta penalmente rilevante' (2013). Access online: https://www.academia.edu/5445809/La_minaccia_Contributo_allo_studio_delle_modalit%C3%A0_della_condotta_penalmente_rilevante.

S. Greengard, 'Will deepfakes do deep damages?' (2020), 63(1) Communications of the ACM, p.17-19. Access online: https://dl.acm.org/doi/fullHtml/10.1145/3371409.

D. Harris, 'Deepfakes: False Pornography is Here and the Law cannot Protect You' (2019) 17 Duke Law & Technology Review 99. Access online: https://scholarship.law.duke.edu/dltr/vol17/iss1/4/.

A. Hauser, M. Ruef, 'Deepfake - An Introduction'. Access online: https://www.scip.ch/en/?labs.20181004 .

A. Kharel, 'Doctrinal Legal Research' (February 26, 2018). Access online: http://dx.doi.org/10.2139/ssrn.3130525.

T. Kirchengast, 'Deepfakes and image manipulation: criminalization and control', (2020), 29 Information & Communications technology law 3. Access online: https://doi.org/10.1080/13600834.2020.1794615.

B. Maier, 'How has the law attempted to tackle the borderless nature of the Internet?', (2010), 18International Journal of Law and Information Technology, 2. Access online: https://sso.uvt.nl/login?rid=ir82szLnSkVuNbayQ3OcsikF__Km6AT6knjSptuYTw8ABbfDyFhcuUdVWWxlldWjObDCB6xAJc5sAHNpbXBsZXNhbWxwaHAAaHR0cHM6Ly9zYW1sLnV2dC5ubC9tb2R1bGUucGhwL2FzZWxlY3QvY3JlZGVudGlhbHMucGhwP3NzcF9zdGF0ZT1fNWQ0MzMyMjJiNGE1OGM4MjZlMDA5OGFlYzUzNGRkZDIxM2I1NTczNmEyJTNBaHR0cHMlM0ElMkYlMkZzYW1sLnV2dC5ubCUyRnNhbWwyJTJGaWRwJTJGU1NPU2VydmljZS5waHAlM0ZzcGVudGl0eWlkJTNEaHR0cHMlMjUzQSUyNTJGJTI1MkZlbmdpbmUuc3VyZmNvbmV4dC5ubCUyNTJGYXV0aGVudGljYXRpb24lMjUyRnNwJTI1MkZtZXRhZGF0YSUyNmNvb2tpZVRpbWUlM0QxNjA5NDI2Mzkx&a-select-server=sso.uvt.nl.

A. Medrán, 'In the kingdom of post-truth, irrelevance is the punishment. The Post-truth Era: Reality vs. Perception'. (2017).

E. Meskys, A. Liaudanskas, J. Kalpokiene, P. Jurcys, 'Regulating deep fakes: legal and ethical considerations', (2020) 15 Journal of Intellectual Property Law & Practice, 1. Access online: https://doi.org/10.1093/jiplp/jpz167.

L. Musselli, 'La legge 29 maggio 2017, n. 71 sul cyberbullismo: dal "limbo legale" ad una regolamentazione a carattere preventivo-amministrativo' (2018) Privacy, Minori & Cyberbullismo. Access online: https://ebookcentral.proquest.com/lib/uvtilburg-ebooks/detail.action?docID=5434910.

F. Nesso, 'La condotta tipica nel delitto di estorsione. Contributo alla teoria della violenza e della minaccia nel sistema penale', Dirittifondamentali.it (February 2020). Access online:http://dirittifondamentali.it/wp-content/uploads/2020/06/Nesso-La-condotta-tipica-nel-delitto-di-estorsione.pdf.

P. Pittaro, 'La legge sul cyberbullismo' (2017) Famiglia e diritto. Access online: https://arts.units.it/handle/11368/2907618#.X7o8zhNKhQI.

A. Powell, 'Embodied Harms: Gender, Shame and Technology Facilitated Sexual Violence in Cyberspace', (2014), RMIT University, Melbourne.

B. Romano, 'L'introduzione dell'articolo 612-ter del codice penale in materia di diffusione illecita di immagini o video sessualmente espliciti', (2020) Codice rosso. Commento alla l. 19 luglio 2019 n. 69, in materia di tutela delle vittime di violenza domestica e di genere. Access online: <https://pure.unipa.it/it/publications/lintroduzione-dellarticolo-612-ter-del-codice-penale-in-materia-d.

R. Rosenberg, H. Dancig-Rosenberg, 'Reconceptualizing revenge porn' (2020), 63 Arizona Law Review. Access online:https://poseidon01.ssrn.com/delivery.php?ID=363114095103071024071093087019091100127044006079024031064087070000111116071027085085099050107020030120050071065114118074121107058042000066077118070012093015113076107014011081121114092111113084118121017114010018023106000006004081096121075085121102111097&EXT=pdf

David N. Schiff, in 'Socio-Legal theory: Social Structure and Law' (May 1976). Access online: https://doi.org/10.1111/j.1468-2230.1976.tb01458.x

M. Šepec, 'Revenge Pornography or Non-Consensual Dissemination of Sexually Explicit Material as a Sexual Offence or as a Privacy Violation Offence' (2019) 13(2) International Journal of Cyber Criminology. Access online: https://www.cybercrimejournal.com/MihaSepecVol13Issue2IJCC2019.pdf.

A. Sorrentino, A. Baldry, S. Cacace, 'Cyberbullying in Italy' (2018) International Perspectives on Cyberbullying. Access online: https://link.springer.com/chapter/10.1007%2F978-3-319-73263-3_10.

L. Strahilevitz, 'Consent, Aesthetics, and the Boundaries of Sexual Privacy' (2005) University of Chicago Law School Journal.

S. Suwajanakorn, S. Seitz, I Kemelmacher-Shlizerman 'Synthesizing Obama: Learning Lip Sync from Audio' (2017), 36 ACM Transaction on Graphics. Access online: https://grail.cs.washington.edu/projects/AudioToObama/siggraph17_obama.pdf.

T. Taylor, 'Extreme celebrity stalking in the digital age', Face Magazine (18th October 2019). Access online: https://theface.com/culture/celebrity-stalking-harry-styles-taylor-swift-ena-matsuoka-miley-cyrus.

K. Tero, T. Aila, S. Laine, J. Lehtinen. 'Progressive Growing of GANs for Improved Quality, Stability, and Variation' (2017).
C. Vaccari, A. Chadwick, 'Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty and Trust in News', (2020), Social Media + Society. Access online: https://journals.sagepub.com/doi/pdf/10.1177/2056305120903408.

L. Vandenbosch, J. Van Oosten, 'The Relationship Between Online Pornography and the Sexual Objectification of Women: The Attenuating Role of Porn Literacy Education' (2017) 67 Journal of Communication, p. 1015-1036. Access online: https://academic.oup.com/joc/article-abstract/67/6/1015/4753857?redirectedFrom=fulltext.

A. Von Hirsch, A. Bottoms, E. Burney, P. Wikström, 'Criminal Deterrence and Sentence Severity: An Analysis of Recent Research' (2009) 39(2) Alberta Law Review.

A. Waldman, 'A Breach of Trust: Fighting Nonconsensual Pornography', (2017) 102 Iowa Law Review 709, p.10.

M. Westerlund, 'The Emergence of Deepfake Technology: A Review' (2019) 9 Technology Innovation Management Review 39. Access online: https://timreview.ca/sites/default/files/article_PDF/TIMReview_November2019%20-%20D%20-%20Final.pdf.

P. Wright, E. Donnerstein, 'Sex Online: Pornography, Sexual Solicitation, and Sexting' (2014), 25(3) Adolescent Medicine: State of the Art Reviews.

D. Yadav, S. Salmani, 'Deepfake: A Survey on Facial Forgery Technique Using Generative Adversarial Network', (2019), International Conference on Intelligent Computing and Control Systems (ICCS).

G. Ziccardi, 'Cyberstalking and electronic devices: relevant legal-informatics issues' (2012) 6 Italian Journal of Criminology. Access online: https://ojs.pensamultimedia.it/index.php/ric/article/view/516/499.

Case law

Corte di Cassazione civile, section. I, no. 5259 of 18/10/1984.

ECHR 15 January 2009, case 1234/05 (Reklos and Davourlis v. Greece).

Corte di cassazione civile, section III, no.10957 of 06 May 2010.

Corte di Cassazione penale, section VI, no. 32404 of 16/07/2010.

Corte di Cassazione penale, section V no. 8193 of 14/01/2012.

ECJ 13 May 2014, ECLI:EU:C:2014:317 (Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González).

Corte di Cassazione penale, section I, no. 37596 of 12/09/2014.

Corte di Cassazione penale, section V, no. 8328 of 13/07/2015.

Corte di Cassazione penale, section II, no. 22265 of 13/01/2017.

Tribunale di Pordenone, section Civile, sentenza no. 634 of 29 August 2017.

Corte di Cassazione penale, section V, no. 57764 of 28/12/2017.

Consiglio di Stato, section III, no. 2599 of 25/05/2018.

Corte di Cassazione penale, section V no. 35817 of 18/06/2018.

Corte di Cassazione penale, section V, no. 36076 of 27/07/2018.

Corte di Cassazione penale, section III, no. 19659 of 19/01/2019.

Corte d'appello di Campobasso, section Civile, sentenza no 84 of 21 February 2019.

Corte di Cassazione penale, section V no. 17159 of 20/03/2019.

Tribunale di Bari, Sez. I Civile, ordinanza no. 5359 of 7 November 2019.

Reports

CLUSIT Report on CyberSecurity in Italy, (2020). Access online: https://d110erj175o600.cloudfront.net/wp-content/uploads/2020/03/Rapporto-Clusit-2020.pdf.

European Parliament, Directorate General for internal policies, The Policy on Gender Equality in Italy, (2014). https://www.europarl.europa.eu/RegData/etudes/note/join/2014/493052/IPOL-FEMM_NT(2014)493052_EN.pdf.

Technical Report of the Survey of Adult Skills (PIAAC), (2013) https://www.oecd.org/skills/piaac/_Technical%20Report_17OCT13.pdf.

Autorità Garante per la Protezione dei dati personali (Italian Data Protection Authority), 'Deepfake. Il falso che ti ruba la faccia (e la privacy)', (December 2020). Access online:

https://www.garanteprivacy.it/documents/10160/0/Deepfake+-+Vademecum.pdf/478612c7-475b-2719-417f-869e5e66604e?version=2.0.

News articles

H. Ajder, G. Patrini, F. Cavalli, L.Cullen, 'The State of Deepfakes' (2019). Access online: https://deeptracelabs.com/mapping-the-deepfake-landscape

L. Alpatrum, 'Deepfake Porn Harms Adult Performers, too', Wired Magazine, (15th January 2020). Access online: https://www.wired.com/story/deepfake-porn-harms-adult-performers-too/

S. Barr, 'David Beckham appeals for end to malaria by 'speaking' in nine languages', the Independent (9th April 2019). Access online: https://www.independent.co.uk/life-style/health-and-families/david-beckham-malaria-must-die-campaign-disease-nine-languages-a8861246.html.

R. Chatterjee, 'I Couldn't Talk or Sleep for Three Days': Journalist Rana Ayyub's Horrific Social Media Ordeal over Fake Tweet,', MSN (28th April 2018). Access online: https://www.msn.com/en-in/news/newsindia /%E2%80%98i-couldn%E2%80%99t-talk-or-sleep-for-three-days%E2%80%99-journalist

R. Chesney & D. Citron, 'Deep Fakes and the New Disinformation War: The Coming Age of Post-Truth Geopolitics', Foreign Affairs. (Jan./Feb. 2019). Access online: https://www.foreignaffairs.com/articles/world/2018-12-11/deepfakes-and-new-disinformation-war.

S. Cole, 'AI-Assisted Fake Porn Is Here and We're All Fucked', MOTHERBOARD (2017). Access online: https://motherboard.vice.com/en_us/article/gydydm/gal-gadot-fake-ai -porn.

S. Cole, 'Deepfakes Were Created as a Way to Own Women's Bodies—We Can't Forget That', Vice Magazine (19th June 2018). Access online: https://www.vice.com/en_ca/article/j5kk9d/deepfakes-were-created-as-a-way-to-own-womens-bodieswe-cant-forget-that-v25n2.

N. Cottone, 'La manipolazione dei video si presta a crimini gravissimi', Il Sole 24Ore, (24th October 2019). Access online: https://www.ilsole24ore.com/art/deepfake-manipolazione-video-si-presta-crimini-gravissimi-ACqViOv.

A. Eaton et al., 'Nationwide Online Study of Nonconsensual Porn Victimization and Perpetration', CYBER C.R. INITIATIVE 12 (June 2017). Access online: https://www.cybercivilrights.org/wp -content/uploads/2017/06/CCRI-2017-Research-Report.pdf.

D. Güera, E. J. Delp, 'Deepfake Video Detection Using Recurrent Neural Networks', 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS). (27-30 November 2018). Access online: https://ieeexplore-ieee-org.tilburguniversity.idm.oclc.org/abstract/document/8639163.

D. Harwell, 'Fake-porn videos are being weaponized to harass and humiliate women: everybody is a potential target'. Washington Post (18th December 2019). Access online:

https://www.washingtonpost.com/technology/2018/12/30/fake-porn-videos-are-being-weaponized-harass-humiliate-women-everybody-is-potential-target/?utm_term=.4adcb8ad9ad2.

B. Marr, 'The Best (And Scariest) Examples Of AI-Enabled Deepfakes', Bernard Marr Blog (2020). Access online: https://bernardmarr.com/default.asp?contentID=1927.

K. Melville, 'The insidious rise of deepfake porn videos and one woman who won't be silenced', ABC news Australia. (30th August 2019). Access online: https://www.abc.net.au/news/2019-08-30/deepfake-revenge-porn-noelle-martin-story-of-image-based-abuse/11437774.

T. O'Brien, 'Scarlett Johansson says fighting deepfake porn is 'fruitless', The Washington Post, (2019). Access online: https://www.washingtonpost.com/gdpr-consent/?next_url=https%3a%2f%2fwww.washingtonpost.com%2ftechnology%2f2018%2f12%2f31%2fscarlett-johansson-fake-ai-generated-sex-videos-nothing-can-stop-someone-cutting-pasting-my-image%2f.

R. Rijitano, 'Deepfake su Telegram, c'è un bot che spoglia le donne: quasi 700 mila vittime', Repubblica, (20th October 2020). Access online: https://www.repubblica.it/tecnologia/sicurezza/2020/10/20/news/deepfake_un_bot_sveste_le_donne_oltre_100mila_vittime-271131375/.

K. Roose, 'Here Come the Fake Videos, Too', New York Times (4th March 2018). Access online: https://www.nytimes.com/2018/03/04/technology/fake-videos-deepfakes.html.

A. Schleicher, 'Closing Italy's skills gap is everyone's business', OECD Education and Skills Today, (October 5th 2017). Access online: https://oecdedutoday.com/closing-italys-skills-gap-is-everyones-business/.

N. Schmidt, 'Privacy law and resolving deepfakes online', IAPP blog, (30th January 2019). Access online: https://iapp.org/news/a/privacy-law-and-resolving-deepfakes-online/.

'Texas Outlaws 'Deepfakes'—but the Legal System May Not Be Able to Stop Them', Law.com-Texas Lawyers, (11th October 2019). Access online:https://www.law.com/texaslawyer/2019/10/11/texas-outlaws-deepfakes-but-the-legal-system-may-not-be-able-to-stop-them/?slreturn=20200115124016.

'Tiziana Cantone: Suicide following years of humiliation online stuns Italy', BBC News, (2017). Access online: https://www.bbc.com/news/world-europe-37380704.

S. Venkataramakrishnan, 'Can you believe your eyes? How deepfakes are coming for politics', Financial Times (24th October 2019). Access online: https://www.ft.com/content/4bf4277c-f527-11e9-a79c-bc9acae3b654.

J. Waters, 'Real dangers of virtual child porn', (27th January 2003), The Irish Times. Access online: https://www.irishtimes.com/opinion/real-dangers-of-virtual-child-porn-1.346757 .

B. Yildirim, C. Aydinli, ‘Deepfake: An Assessment from The Perspective of Data Protection Rules’, MONDAQ, (13th November 2019). Access online: https://www.mondaq.com/turkey/privacy-protection/863064/deepfake-an-assessment-from-the-perspective-of-data-protection-rules?.