Regulating Deepfake Technology

Legislative possibilities in the Netherlands to obstruct the use of deepfake technology for the creation of non-consensual pornography

Daphne Stevens
SNR: 2047638

Master's Thesis Law and Technology
Tilburg Law School

Tilburg, 18 May 2020

TFG 8 – Brave New World
Supervisors: Merel Noorman and Silvia de Conca

Word count (excluding table of contents, footnotes, annex and bibliography): 17.015

Table of contents

Chapter 1: Introduction

1.1 Background

Deepfake technology is gaining popularity. A recent report by the cybersecurity company Deeptrace found that the amount of deepfake videos circulating online has almost doubled in less than a year. In December 2018, 7,964 deepfake videos circulated online, while in July 2019 this number increased to 14,678 videos.[1] Deepfake technology can be used to create many different kinds of videos, but using this technology to create pornography is by far the most popular application of this technology. Deeptrace found that 96% of the deepfake videos circulating online contained pornographic content.[2]

1.2 Problem statement

In a news article by the NOS of September 2019, the Dutch Public Prosecution Office expressed its worries about the increasing popularity of deepfake technology.[3] Even though there are many positive applications for this technology, there is also a potential for misuse, such as extorting or conning people. According to the public prosecutor Lodewijk van Zwieten, who was interviewed for the aforementioned news article on this subject, new legislation to deal with this technology was not necessary. Current legislation in the Netherlands would suffice to obstruct the use of deepfake technology with harmful intentions.

The statement that current legislation in the Netherlands suffices to deal with this problem sparked my interest. In many countries, such as the United States and the United Kingdom, there have been calls that the regulation of deepfake technology is necessary, more specifically with regard to the use of this technology for the creation of non-consensual pornography. However, there has been no debate in the Netherlands about whether specifically regulating non-consensual deepfake pornography would be necessary. The Dutch government has expressed the need to educate citizens about disinformation and the manipulation of elections, where deepfake technology plays a role as well.[4] There has been a very limited debate in the Netherlands on this technology specifically. At the time of writing, no debate exists in the Netherlands on non-consensual deepfake pornography and the harmful effects of the creation and publication of these sexual images. I am of the opinion that this debate is necessary, because there have been different cases of non-consensual deepfake pornography in the Netherlands, with examples of Dionne Stax and Bridget Maasland being portrayed in deepfake pornography.[5] Furthermore, no research has been published whether the current Dutch legislation is actually sufficient to obstruct this harmful use of the technology.

---

[1] Deeptrace, 'The State of Deepfakes' (2019), p. 1. Access online: https://storage.googleapis.com/deeptrace-public/Deeptrace-the-State-of-Deepfakes-2019.pdf (last accessed on 18 April 2020).
[2] Deeptrace, 'The State of Deepfakes' (2019), p. 1. Access online: https://storage.googleapis.com/deeptrace-public/Deeptrace-the-State-of-Deepfakes-2019.pdf (last accessed on 18 April 2020).
[3] J. Schellevis, 'Zorgen OM over deepfakes: "Risico op oplichting en afpersing"' (7 September 2019) NOS. Access online: https://nos.nl/artikel/2300688-zorgen-om-over-deepfakes-risico-op-oplichting-en-afpersing.html (last accessed on 18 April 2020).
[4] K.H. Ollongren, 'Brief inzake desinformatie en beïnvloeding verkiezingen' (2018). Access online: https://www.rijksoverheid.nl/documenten/kamerstukken/2018/12/13/kamerbrief-over-dreiging-desinformatie-en-beinvloeding-verkiezingen (last accessed on 25 April 2020).
[5] T. Tates, 'Manager woest na opduiken deepfake-pornofilmpje Dionne Stax: "Aangifte in voorbereiding"' (27 August 2019) AD. Access online: https://www.ad.nl/binnenland/manager-woest-na-opduiken-deepfake-pornofilmpje-dionne-stax-aangifte-in-voorbereiding~af9dace5/ (last accessed on 28 April 2020); Shownieuws, 'Bridget Maasland slachtoffer van deepfake-porno' (4 March 2020) Shownieuws. Access online: https://www.shownieuws.nl/video/clips/2020/bridget-slachtoffer/ (last accessed on 13 May 2020).

In order to start a debate regarding the regulation of deepfake technology that is used to create non-consensual pornography and to research whether the current legislation in the Netherlands can be used to regulate deepfake technology, my thesis will focus on the regulation of deepfake technology. There is a broad range of applications of this technology, but my research will solely focus on the use of deepfake technology to create non-consensual pornography. Having a specific focus on non-consensual deepfake pornography is important, because deepfake technology is mainly used to create pornography.[6] Furthermore, non-consensual pornography can have severely harmful effects on the people who are portrayed in the pornography. Because of the easy applicability of this technology, everyone could potentially fall victim to this and be portrayed in non-consensual deepfake pornography.[7]

1.3 Existing research on deepfake technology

There are different academic articles that discuss the problems created by deepfake technology. The main point of view is that even though there are many beneficial uses of deepfake technology, such as its uses for education, art and self-expression, there are also harmful uses of the technology that need to be halted.[8] Examples of harmful uses are exploitation, reputational sabotage, influencing elections and undermining journalism by spreading disinformation.[9]

Deepfake technology that is used to create non-consensual pornography brings different challenges.[10] One of these challenges is the issue of identifying the crime, because it is difficult to determine and prove the harm caused by non-consensual deepfake pornography.[11] Furthermore, it is difficult to identify the perpetrator, because of the anonymity that the Internet provides.[12] Seeking recourse is a challenge as well, because many provisions do not offer the possibility to get content removed from the Internet, and when this is possible, it is difficult to get the content removed from the Internet completely.[13]

The existing literature on the regulation of deepfake technology focusses specifically on the United States, where current legislation is deemed insufficient by different authors.[14] The general consensus is that current legislation in the United States is insufficient, because non-consensual deepfake pornography does not fall under the scope of different provisions. The reason for this is that non-consensual deepfake pornography is virtual and therefore it is difficult to prove harm, which is an important element when proving for example the

---

[6] Deeptrace, 'The State of Deepfakes' (2019), p. 1. Access online: https://storage.googleapis.com/deeptrace-public/Deeptrace-the-State-of-Deepfakes-2019.pdf (last accessed on 18 April 2020).
[7] R.A. Delfino, 'Pornographic Deepfakes – Revenge Porn's Next Tragic Act – The Case for Federal Criminalization' (2019) 88 Fordham Law Review 887, p. 893 & 898.
[8] B. Chesney & D. Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy and National Security' (2019) 107 California Law Review 1753.
[9] B. Chesney & D. Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy and National Security' (2019) 107 California Law Review 1753.
[10] R.A. Delfino, 'Pornographic Deepfakes – Revenge Porn's Next Tragic Act – The Case for Federal Criminalization' (2019) 88 Fordham Law Review 887.
[11] D. Harris, 'Deepfakes: False Pornography is Here and the Law cannot Protect You' (2019) 17 Duke Law & Technology Review 99, p. 121.
[12] R.A. Delfino, 'Pornographic Deepfakes – Revenge Porn's Next Tragic Act – The Case for Federal Criminalization' (2019) 88 Fordham Law Review 887, p. 898-899.
[13] R.A. Delfino, 'Pornographic Deepfakes – Revenge Porn's Next Tragic Act – The Case for Federal Criminalization' (2019) 88 Fordham Law Review 887, p. 898-901.
[14] D. Harris, 'Deepfakes: False Pornography is Here and the Law cannot Protect You' (2019) 17 Duke Law & Technology Review 99; R.A. Delfino, 'Pornographic Deepfakes – Revenge Porn's Next Tragic Act – The Case for Federal Criminalization' (2019) 88 Fordham Law Review 887.

Intentional Infliction of Emotional Distress.[15] Different criminal provisions in the United States also require an intent to cause harm when publishing non-consensual pornography, which is difficult to prove.[16] It is difficult to prove harm because one can easily argue that it is just virtual footage, and not something that has taken place and harmed the victim in real life. Furthermore, in some cases damages are possible, but there is no possibility to get the sexual image deleted from the internet.[17] There are calls in the United States to create specific legislation to criminalize the creation and publication of non-consensual deepfake pornography.[18] Different states in the United States have responded to these calls through the creation of specific legislation, such as the state of Virginia.[19] The legal scholars Chesney and Citron have brought forward other solutions as well, such as technological responses and market solutions.[20]

There is a lack of focus on Europe, even though the issue of non-consensual deepfake pornography is present there as well.[21] Research has been conducted and published in Europe that is focussed on non-consensual pornography.[22] However, no academic literature on non-consensual deepfake pornography exists, even though the application of legislation may be different for this type of virtual pornography than it is for other types of non-consensual pornography, because the sexual act has not taken place in real life and therefore the argument could be made that the impact of it is not as big as the creation and publication "real" sexual images. The impact that the virtual pornography has on the victim may be different, and therefore prosecutors may look at it differently. Research focussed on Europe is important, because legislation in Europe is different than in the United States. There might be provisions in European countries that may be sufficient to deal with non-consensual deepfake pornography. Researching whether existing legislation can be applicable to non-consensual deepfake pornography is useful, because it creates new insights into how one can properly deal with cases of non-consensual deepfake pornography through legislation. My thesis will fill the gap that in the literature on this topic within Europe by focussing my research on the Netherlands. This can be a starting point for further research, both within the Netherlands and in other European countries.

[15] D. Harris, 'Deepfakes: False Pornography is Here and the Law cannot Protect You' (2019) 17 Duke Law & Technology Review 99, p. 111-112.
[16] D. Harris, 'Deepfakes: False Pornography is Here and the Law cannot Protect You' (2019) 17 Duke Law & Technology Review 99, p. 121.
[17] D. Harris, 'Deepfakes: False Pornography is Here and the Law cannot Protect You' (2019) 17 Duke Law & Technology Review 99, p. 118.
[18] D. Harris, 'Deepfakes: False Pornography is Here and the Law cannot Protect You' (2019) 17 Duke Law & Technology Review 99.
[19] Code of Virginia, §18.2-362.2 'Unlawful dissemination or sale of images of another; penalty'. Access online: https://law.lis.virginia.gov/vacode/18.2-386.2/ (last accessed on 18 April 2020).
[20] B. Chesney & D. Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy and National Security' (2019) 107 California Law Review 1753.
[21] T. Tates, 'Manager woest na opduiken deepfake-pornofilmpje Dionne Stax: "Aangifte in voorbereiding"' (27 August 2019) AD. Access online: https://www.ad.nl/binnenland/manager-woest-na-opduiken-deepfake-pornofilmpje-dionne-stax-aangifte-in-voorbereiding~af9dace5/ (last accessed on 28 April 2020).
[22] M. Goudsmit, 'Criminalising Image-based Sexual Abuse: an Analysis of the Dutch Bill against Revenge Pornography' (2019) 68 Ars Aequi 442; S. van der Hof, 'Wraakporno op Internet' (2016) 65 Ars Aequi 54.

1.4 Main research question

The main research question for my thesis is the following question:

> *What are the legislative possibilities for the government of the Netherlands to obstruct the use of deepfake technology for the creation of non-consensual pornography?*

1.5 Sub-questions

In order to answer the main research question, I have formulated five sub-questions that I will answer during my research.

1. What is deepfake technology and how can this technology be used to create non-consensual pornography?
2. What are the societal, ethical and legal issues connected to the use of deepfake technology for the creation of non-consensual pornography?
3. In what manner can existing regulation in the Netherlands play a role in obstructing the use of deepfake technology for the creation of non-consensual pornography?
4. Does non-consensual deepfake pornography fall under the scope of current legislation in the Netherlands or are there gaps in the legislation when it is used to obstruct the use of deepfake technology for the creation of non-consensual pornography?
5. If there are gaps in the current legislation, what are possible solutions to fill these gaps in the legislation?

1.6 Methodology and methods

My research question is a combination of a descriptive question and an evaluative question. I will describe the different legislative possibilities to obstruct the use of deepfake technology for the creation of non-consensual pornography that are already existing in the current legislation in the Netherlands and evaluate these legislative possibilities.

My methodology to answer the research question is a combination of doctrinal legal research and a review of secondary literature. Through doctrinal legal research I am able to find the legislation and case law that could possibly be applicable in cases of non-consensual deepfake pornography. Through primary and secondary sources regarding the legislation that could possibly be applicable, I can analyse how the law is formulated in order to assess whether non-consensual deepfake pornography falls within the scope of the legislation. When assessing the current legislation, I will look at the legislation itself, explanatory reports and case law. I will assess whether non-consensual deepfake pornography falls within the scope of the legislation that could possibly be used in cases regarding non-consensual deepfake pornography. Furthermore, I will look at the legal redress that these different provisions offer, and check whether this would meet the needs of the victims of non-consensual deepfake pornography. Here I will for example assess whether the legislation offers a recourse to get the content removed from the Internet.

Provisions that I will discuss are the criminal provisions regarding child pornography, revenge pornography, insult and crimes against personal freedom, the portrait right (article 21 Auteurswet) and the right to be forgotten from the Algemene Verordening Gegevensbescherming. The legislation that I will research is the legislation that I consider to be possibly applicable to non-consensual deepfake pornography. I have gained the knowledge which legislation could possibly be used through research of Dutch literature on revenge pornography and academic literature on the regulation of non-consensual deepfake

pornography in the United States. With this knowledge I have selected the provisions where non-consensual deepfake pornography may fall within the scope, in order to research these provisions in more detail.

The current legislation in the Netherlands will be further assessed from a socio-legal perspective. I will draw on literature from the fields of victimology and criminology. The focus on these fields enables me to explain the effects that non-consensual pornography has on victims. Furthermore, it enables me to research the effects that the legislation has on victims, when it comes to seeking recourse, and perpetrators, when it comes to being deterred to act in a certain manner. Based on this analysis, I will evaluate the Dutch provisions that could be used when dealing with deepfake technology and bring forward eventual recommendations, such as whether existing legislation needs to be changed or new legislation needs to be introduced.

My chosen methods to answer my main research-question and sub-questions are academic literature research and a study of legal texts and case law. Through the study of legal texts and case law I can assess which current laws can be used to regulate the use of deepfake technology for the creation of non-consensual pornography. Academic literature research will play a role in this as well. It enables me to gain insights in the technology and its effects, and the different pieces of Dutch legislation and their scope. With these insights, I can explain deepfake technology and its effects, and evaluate the currently existing legislation in the Netherlands in the manner that I discussed in the prior paragraphs.

1.7 Structure

In the second chapter I will discuss deepfake technology and non-consensual pornography. Here I will answer the sub-question 1 and a part of sub-question 2. Firstly, I will explain what deepfake technology entails. Furthermore, I will explain how this technology is used to create non-consensual pornography. I will then discuss the benefits and harms of deepfake technology. Lastly, I will specifically focus on the issues that arise in connection to non-consensual deepfake pornography, in order to show why non-consensual deepfake pornography deserves attention on its own.

In the third chapter, I will discuss different provisions of the Dutch Criminal Code and assess whether non-consensual deepfake pornography falls under the scope of these provisions. In this chapter and in the following chapter I will answer a part of sub-question 2, sub-question 3 and a part of sub-question 4.

In the fourth chapter, I will assess two other pieces of legislation: the portrait right of the Dutch Copyright Law and the right to be forgotten of article 17 of the General Data Protection Regulation. I will research whether these laws can be used in cases of non-consensual deepfake pornography.

In the fifth chapter I will answer the final part of the fourth and the fifth sub-question. Here I will conclude whether the provisions examined in chapter 3 and 4 can be used in cases of non-consensual deepfake pornography. Based on the analysis, I conclude that the existing legislation in the Netherlands can be used in cases of non-consensual deepfake pornography, but clarification through case law and legislation itself is necessary in order to fill the gaps and clarify uncertainties.

The sixth chapter will contain the conclusion of the thesis.

Chapter 2: Non-consensual deepfake pornography

2.1 Introduction

In sections 2.2 to 2.4 I discuss what deepfake technology is and how it can be used to create non-consensual pornography. The beneficial and harmful impacts of deepfake technology are discussed in sections 2.5 to 2.7. In section 2.8 I will specifically focus on the issues caused by non-consensual deepfake pornography, as this is the type of deepfake that I focus on in my research. Finally, section 2.9 contains a short conclusion on how the Dutch legislator should respond to deepfake technology.

2.2 What is deepfake technology?

Deepfake technology makes it possible to create images, video and audio where people are portrayed doing or saying things that they never said or did. The term deepfake was first used by the Reddit user u/deepfakes, who created a Reddit community of the same name which was dedicated to the use of deep learning software to place the faces of female celebrities in pornographic videos.[23] The name is a mix of the terms 'deep learning' and 'fake', and it describes that deep learning is used to create fake images, video and audio. According to Chesney and Citron, the term deepfake can be used to describe the "full range of hyper-realistic digital falsification of images, video and audio."[24]

Deepfake technology relies on machine learning, which is a form of artificial intelligence. Artificial intelligence are computer models of human behaviour and thought processes, which are designed to simulate human behaviour in order to design digital technologies that can for example solve difficult problems.[25] Machine learning allows computer systems to learn from data and carry out complex processes with the knowledge that they gained from these data, instead of working in a pre-programmed manner.[26]

Different machine learning techniques can be used to create deepfakes, but the General Adversarial Network (GAN) currently is the most popular technique.[27] GANs are two artificial neural networks that cooperate to create images and other samples, such as voice samples. An artificial neural network is "a computational model that consists out of several processing elements that receive inputs and deliver outputs based on their predefined activation functions."[28] These two networks, which are called 'the generator' and 'the discriminator', are trained with the same datasets of audio, video and/or images. The generator creates new media, where it tries to create samples of such a quality that these cannot be distinguished from real media. These new samples are passed on to the discriminator, together with real media taken from the original dataset. The discriminator then evaluates the input data for authenticity and determines whether the samples can or cannot be

---

[23] Deeptrace, 'The State of Deepfakes' (2019), p. 3. Access online: https://storage.googleapis.com/deeptrace-public/Deeptrace-the-State-of-Deepfakes-2019.pdf (last accessed on 18 April 2020).
[24] B. Chesney & D. Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753, p. 1757.
[25] M-H. Maras & A. Alexandrou, 'Determining the authenticity of video in the age of artificial intelligence and in the wake of Deepfake videos' (2019) 23 The International Journal of Evidence & Proof 255, p. 256.
[26] M-H. Maras & A. Alexandrou, 'Determining the authenticity of video in the age of artificial intelligence and in the wake of Deepfake videos' (2019) 23 The International Journal of Evidence & Proof 255, p. 256.
[27] Deeptrace, 'The State of Deepfakes' (2019), p. 3. Access online: https://storage.googleapis.com/deeptrace-public/Deeptrace-the-State-of-Deepfakes-2019.pdf (last accessed on 18 April 2020).
[28] F. Eshragh *et al.*, 'Automated negotiation in environmental resource management: Review and assessment' (2015) 162 Journal of Environmental Management 148, p. 152.

discerned from real media. The discriminator then gives feedback to the generator, with which the generator can learn and improve its outcome even further.[29]

In order to create deepfakes, the GANs are fed datasets of the footage that will be portrayed, which can for example be a movie, a pornographic image or a recording of speech. Furthermore, the GANs are also fed datasets containing images, videos or voice recordings of the person who will eventually be portrayed in the video, picture or voice recording. The source material can consist of footage of celebrities, but also of non-famous people.[30] In the age of social media, it is easy to access great amounts of photographs and videos from any person. This can for example be used as source material of someone's face structure and facial expressions in order to create a deepfake of that person.[31] Because of this, it is possible to create a deepfake of any person, as long as there is enough source material to train the GANs with. Research has shown that roughly 500 pictures are needed in order to create a realistic deepfake, but this also depends on the length of the deepfake that you create.[32] With less images it is still possible to create a deepfake, but it will look less realistic.

Deepfakes and deepfake creation software are becoming increasingly accessible. There are deepfake computer apps, which can be downloaded to create deepfakes. Different software is available to download for free, and many tutorials for the creation of deepfakes can be found online.[33] Furthermore, there are service portals which generate and sell custom deepfakes. Someone uploads footage of the person who they want to be portrayed in the deepfake to an online platform, where the deepfake is generated afterwards by the person who offers their services on the portal. Lastly, there are forums and online marketplaces where individual deepfake creators offer their services.[34] Because there is such a great volume of deepfake technology services, which are quite sophisticated, a steady diffusion of deepfakes is ensured.[35]

2.3 What is non-consensual pornography?

According to Danielle Citron, non-consensual pornography "involves the distribution of sexually graphic images without the consent of the person who is portrayed in these images."[36] This term is quite broad and involves the distribution of sexually graphic images

---

[29] M. Westerlund, 'The Emergence of Deepfake Technology: A Review' (2019) 9 Technology Innovation Management Review 39, p. 40-41; I.J. Goodfellow *et al.*, 'General Adversarial Nets' (2014) 2 NIPS'14: Proceedings of the 27th International Conference on Neural Information Processing Systems 2672.

[30] C. Öhman, 'Introducting the pervert's dilemma: a contribution to the critique of Deepfake Pornography' (2019) Ethics and Information Technology, p. 1-2. Access online: https://rdcu.be/b3DZM (last accessed on 18 April 2020).

[31] K. Farish, 'Do deepfakes pose a golden opportunity? Considering whether English law should adopt California's publicity right in the age of deepfake' (2020) 15 Journal of Intellectual Property Law & Practice 40, p. 42.

[32] A. Hauser, 'Deepfake Analysis: Amount of Images, Lighting and Angles' (22 November 2018) SCIP. Access online: https://www.scip.ch/en/?labs.20181122 (last accessed on 13 May 2020).

[33] K. Farish, 'Do deepfakes pose a golden opportunity? Considering whether English law should adopt California's publicity right in the age of deepfake' (2020) 15 Journal of Intellectual Property Law & Practice 40, p. 41.

[34] Deeptrace, 'The State of Deepfakes' (2019), p. 4-5. Access online: https://storage.googleapis.com/deeptrace-public/Deeptrace-the-State-of-Deepfakes-2019.pdf (last accessed on 18 April 2020).

[35] B. Chesney & D. Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753, p. 1763.

[36] D. Citron, 'Sexual Privacy' (2018) 25 University of Maryland Francis King Carey School of Law Legal Studies Research Paper 1870, p. 1917. Available on SSRN: http://ssrn.com/abstract=3233805 (last accessed on 18 April 2020).

that were obtained without consent, but also images originally obtained with consent.[37] According to the legal scholar Goudsmit, feigned pornography that is published without the portrayed person's consent also falls within the scope of the term non-consensual pornography in the Netherlands.[38] Feigned pornography is the type of pornography where someone's face is placed on the body of another person who is engaged in sexual activities, which makes it seem as if the portrayed person is engaged in the activity. Deepfake pornography seems to fall within the scope of this term.

In this thesis, the definition of non-consensual pornography is as follows: sexually graphic images or videos, whether real or feigned, which are created and/or distributed without the consent of the person (or persons) who is (are) portrayed in the images or videos.

2.4 How can deepfake technology be used to create non-consensual pornography?

Deepfake technology is used to create non-consensual pornography. In order to do this, the neural networks that create the deepfakes are fed datasets containing pornographic material and footage of the person whose face will be placed in the video. The existing pornographic material is then modified by the technology to swap out the face of the performer with the face of another person.[39]

A significant majority of the deepfake videos that are created and circulating online are pornographic deepfakes.[40] Websites such as Twitter, Pornhub and Reddit have banned pornographic deepfake videos.[41] These bans have led to the launch of different websites that allow users to create and share deepfake videos, including deepfake pornography.[42] Examples of these websites are Deepfakes Web[43] and MachineTube[44]. In turn, these websites have led to a sophistication of deepfake technology, because on those websites it is easier to get in contact with others who create and share deepfake videos. These websites make deepfake technology accessible for everyone, giving them the opportunity to create videos and develop their skills. The websites also provide users with the possibility to share their creations with other users, which thus makes it easier to share content. This has a big effect on the reach of deepfake technology, which will be further explained in the following section.

---

[37] S.R. Stroud & J. Henson, 'What Exactly is Revenge Porn or Nonconsensual Pornography?' (2016), p. 1. Available on SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2828740 (last accessed on 18 April 2020).

[38] M. Goudsmit, 'De wijzende vinger bekeken: Over de strafbaarstelling van wraakpornografie' (2018) 24 NJB 1721, p. 1722.

[39] T. Wagner & A. Blewer, '"The World Is No Longer Real": Deepfakes, Gender, and the Challenges of AI-Altered Video' (2019) 3 Open Information Science 32, p. 37.

[40] Deeptrace, 'The State of Deepfakes' (2019), p. 6. Access online: https://storage.googleapis.com/deeptrace-public/Deeptrace-the-State-of-Deepfakes-2019.pdf (last accessed on 18 April 2020).

[41] H.K. Hull, 'When Seeing Isn't Believing' (2019) 27 Catholic University Journal of Law and Technology 51, p. 57.

[42] C. Öhman, 'Introducting the pervert's dilemma: a contribution to the critique of Deepfake Pornography' (2019) Ethics and Information Technology, p. 2. Access online: https://rdcu.be/b3DZM (last accessed on 18 April 2020).

[43] Deepfakes Web, https://deepfakesweb.com/ (last accessed on 13 May 2020).

[44] MachineTube, https://www.machine.tube/ (last accessed on 13 May 2020).

2.5 The reach of deepfake technology

The sophistication and availability of deepfake technology that was touched upon in the prior sections has a big effect on the scale on which this technology is used. Almost anyone who owns a computer is able to create deepfake videos that are practically indistinguishable from reality.[45]

Besides the availability and sophistication of the technology, global connectivity plays an important role in the reach of deepfake technology as well. Global connectivity, such as through social media, makes it easier to distribute content. Because there is such a large amount of content that is distributed online, there is much less screening of this content. The overall amount of gatekeeping has reduced, because so much footage is posted online that moderators cannot assess everything.[46] Because of this, different kinds of content, even inaccurate content, can easily reach big audiences. Content that is placed online can circulate far and wide.[47] False and shocking content is more likely to be shared on social media, which further accounts to the wide and rapid spread of deepfake videos, and more specifically deepfake pornography.[48] In this manner, deepfake videos can be spread over the Internet, leaving its traces everywhere and making it practically impossible to fully delete the content from the Internet. The ease of copying and storing data online also plays an influential role here.

Improved search possibilities also play a role on the reach of deepfake technology. It is easier to find information and footage of persons, for example through more precise search results and the possibility of reverse image search. With reverse image search you can provide a photo to Google Image Search or another website that offers reverse image search, where it searches for similar photos. This makes it easier to collect enough source material of a person to create a realistic-looking deepfake. Furthermore, when the content is created and placed online, it is easier to find this content online due to the improved search possibilities.[49] One simple search of the name of a person can already bring up deepfake content connected to them.

When discussing the reach of deepfake technology, and more precisely deepfake pornography, it is important to point out that there is an incalculable number of potential victims. Anyone who has ever digitally captured their image could already become a victim of deepfake pornography.[50] In the age of social media, it is easy to access photographs and videos of a person. These materials may be used as source material for a deepfake video.[51] Because of this, a deepfake can be created of practically every person.

---

[45] M. Westerlund, 'The Emergence of Deepfake Technology: A Review' (2019) 9 Technology Innovation Management Review 39, p. 39.
[46] J. Koebler & J. Cox, 'The Impossible Job: Inside Facebook's Struggle to Moderate Two Billion People' (23 August 2018) VICE Motherboard. Access online: https://www.vice.com/en_us/article/xwk9zd/how-facebook-content-moderation-works (last accessed on 26 April 2020).
[47] B. Chesney & D. Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753, p. 1764-1768.
[48] S. Vosoughi *et al.*, 'The spread of true and false news online' (2018) 359 Science 1146.
[49] B. Chesney & D. Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753, p. 1774.
[50] R.A. Delfino, 'Pornographic Deepfakes – Revenge Porn's Next Tragic Act – The Case for Federal Criminalization' (2019) 88 Fordham Law Review 887, p. 893 & 898.
[51] K. Farish, 'Do deepfakes pose a golden opportunity? Considering whether English law should adopt California's publicity right in the age of deepfake' (2020) 15 Journal of Intellectual Property Law & Practice 40, p. 42.

2.6 Benefits of deepfake technology

Deepfake technology has different benefits that encourage the use of this technology. Firstly, the technology can be used to improve education. It gives educators the possibility to provide students with information in other manners than readings and lectures.[52] Seeing a historical person speak about a certain historical event that they have partaken in may be much more interesting and memorable than just a plain reading about that event.

Secondly, there are different artistic benefits when using this technology. It gives artists the possibility to create realistic content where public figures can be satirized, parodied and criticized. Furthermore, activists can use the technology to show their views in a manner that words alone could not.[53]

Deepfake technology can have many positive uses in different industries. It can be used to create special effects in movies and TV shows. It can also create the possibility for realistic voice dubbing for movies in any language, which gives the possibility for a bigger audience to enjoy the movie. Similarly, the technology can break language barriers on video conference calls by translating the speech and altering the facial movements to match up with the translated language. In this way, everyone seems to be speaking the same language, which makes communication easier and more natural. This is not only useful for companies, but also for other online interactions. Deepfake technology can also transform e-commerce and advertising in significant ways.[54] There are different examples of this, such as giving the ability to quickly try on clothes online and providing unique artificial voices with which companies can distinct themselves more easily.

2.7 Harms of deepfake technology

Besides the different benefits that deepfake technology offers, there are also different harms that the technology can cause. These harms can have an effect on different levels, namely on a personal level and on a societal level.

Deepfakes can be used as mechanisms to exploit and sabotage persons. Someone's identity can be stolen, in order to gain financial or some other benefit. Deepfake videos can also be used to abuse a person, by using the identity of a person to harm them or those around them. By falsely portraying a person performing an unacceptable or embarrassing act in a video, a person's reputation can be damaged.[55]

Deepfake pornography can be seen as a type of abusive use of deepfake technology. An example of this can be found in a case where a pornographic deepfake of the Indian investigative journalist Rana Ayyub was placed on different social media platforms with the aim to discredit her work and humiliate her into silence. This led to harassment and 'doxxing', which is the practice revealing of personal information online.[56] The issues of this specific kind of deepfake will be further discussed in section 2.8.

---

[52] B. Chesney & D. Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753, p. 1769-1770.
[53] B. Chesney & D. Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753, p. 1770.
[54] M. Westerlund, 'The Emergence of Deepfake Technology: A Review' (2019) 9 Technology Innovation Management Review 39, p. 41.
[55] B. Chesney & D. Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753, p. 1771-1775.
[56] V. Turk, 'Deepfakes are already breaking democracy. Just ask any woman.' (18 November 2019) WIRED. Access online: https://www.wired.co.uk/article/deepfakes-pornography (last accessed on 16 April 2020).

On a societal level, deepfake technology could harm democracy. With deepfake technology, propaganda can easily be created. This can put politicians or authorities in a bad light, which can have harmful effects. For example, footage can be spread of a politician, showing unacceptable behaviour. This is not real footage, but created with deepfake technology.[57] An example of this can be found in the form of a 'shallowfake', footage that is created with basic editing tools or through placing it out of context, of Nancy Pelosi, whose voice audio was manipulated in order to make her seem slurring her words. This was retweeted by President Trump, and many people left negative comments on the video.[58] This is just a slight change, which already led to people being negative about the congresswoman. There have been no cases yet where actual deepfake technology has been used, but the effects of this may be even greater. According to Chesney and Citron, when this footage would be spread right before elections take place, it may cause interference with these elections when the deepfake footage is believed to be real and voters decide not to vote for that politician anymore due to what they have seen in that footage.[59] Furthermore, citizens may start distrusting information by authorities, either because these authorities are portrayed in a negative manner in a deepfake, or because of the fear that these authorities might spread false information through deepfakes.[60]

Deepfake technology could also affect journalism. Consumers could distrust news stories due to doubts whether certain footage is real or created with deepfake technology.[61] Furthermore, it may create doubts among journalists themselves. Can the authenticity of video or audio evidence of a newsworthy event that is provided by someone be trusted? This is not a new question, but it will be more difficult to answer this question now that deepfake technology has become more sophisticated and popular to use.[62] The same can be said for court cases. There may be doubts whether images, videos or audio can still be used as reliable evidence.

Lastly, there is a harm that is created by the mere existence of the technology. It will be easier to deny the truth due to the existence of deepfake technology. Persons can state that footage of certain acts that they have committed are created with deepfake technology and thus are fake, even though the footage is real. Because it can be difficult to distinguish deepfakes from real footage, this statement may actually be believed.[63] An example of this can be found in Malaysia, a country where same-sex sexual activity is illegal. A sex tape was leaked, showing a male politician and another man engaged in sexual activity. The politician then stated that the video was a deepfake made to sabotage his political career. Experts have

---

[57] M. Westerlund, 'The Emergence of Deepfake Technology: A Review' (2019) 9 Technology Innovation Management Review 39, p. 42.
[58] Deeptrace, 'The State of Deepfakes' (2019), p. 11. Access online: https://storage.googleapis.com/deeptrace-public/Deeptrace-the-State-of-Deepfakes-2019.pdf (last accessed on 18 April 2020).
[59] B. Chesney & D. Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753, p. 1778-1779.
[60] M. Westerlund, 'The Emergence of Deepfake Technology: A Review' (2019) 9 Technology Innovation Management Review 39, p. 42-43; B. Chesney & D. Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753, p. 1779.
[61] M. Westerlund, 'The Emergence of Deepfake Technology: A Review' (2019) 9 Technology Innovation Management Review 39, p. 42.
[62] B. Chesney & D. Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753, p. 1784.
[63] B. Chesney & D. Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753, p. 1785-1786.

not found any evidence that the video was manipulated, and it is still unclear to this day whether the video was real or not.[64]

2.8 Issues of non-consensual deepfake pornography

Due to the specific focus of this research on the use of deepfake technology for the creation of non-consensual pornography, it is important to specifically discuss the harms and issues that can be caused by the creation and publication of non-consensual deepfake pornography.

Non-consensual deepfake pornography can have harmful effects on the person who is portrayed in the footage. Firstly, when a person finds out that there is footage of them performing a sexual act, without this even having taken place, it may cause psychological damage. Victims may feel humiliated and scared, losing sense of belonging because they have the feeling that they have been reduced to sex objects.[65] Negative reactions from people around them, which will be discussed in the upcoming paragraph, may fortify these feelings.

Due to the stigma on nude images, deepfake pornography may have negative consequences on a person's reputation. This especially is the case when a viewer may not realize that the video is fake, and thinks that the person has actually engaged in the sexual act and created footage of this.[66] The reputational damage manifests itself in different ways. People may condemn the victim because now there are nude images of them online, for everyone to see, even if this footage is fake. It can have an effect on intimate relationships, because (prospective) partners may not feel comfortable with the existence of sexually explicit images of their partner online. Furthermore, it can create risks to victims' job prospects. Companies may refuse to hire a person because the search results of the applicant's name include nude images of the applicant, or more specifically deepfake pornography. Search results are important to employers.[67] Research has shown that 75% of the employers actively research candidates online, and more than 70% refused to hire someone based on what they found online.[68]

Non-consensual deepfake pornography also creates privacy issues. Victims are denied agency over their intimate lives, because they are shown performing a sexual act that they have never performed.[69] It affects privacy, and more specifically the sexual privacy of a person, because the portrayed person does not have control over what is portrayed and where this is shared.[70] The reason for this is that a person's face can be easily placed in any kind of pornographic video, and anyone who creates such footage can share it easily, without the

---

[64] Deeptrace, 'The State of Deepfakes' (2019), p. 10. Access online: https://storage.googleapis.com/deeptrace-public/Deeptrace-the-State-of-Deepfakes-2019.pdf. (last accessed on 18 April 2020).
[65] B. Chesney & D. Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753, p. 1773.
[66] R.A. Delfino, 'Pornographic Deepfakes – Revenge Porn's Next Tragic Act – The Case for Federal Criminalization' (2019) 88 Fordham Law Review 887, p. 897-898.
[67] D. Citron, 'Sexual Privacy' (2018) 25 University of Maryland Francis King Carey School of Law Legal Studies Research Paper 1870, p. 1927-1928. Available on SSRN: http://ssrn.com/abstract=3233805 (last accessed on 18 April 2020).
[68] M. Fertik, 'Your Future Employer Is Watching You Online. You Should Be, Too' (3 April 2012) Harvard Business Review. Access online: https://hbr.org/2012/04/your-future-employer-is-watchi (last accessed on 26 April 2020).
[69] D. Citron, 'Sexual Privacy' (2018) 25 University of Maryland Francis King Carey School of Law Legal Studies Research Paper 1870, p. 1921. Available on SSRN: http://ssrn.com/abstract=3233805 (last accessed on 18 April 2020).
[70] D. Citron, 'Sexual Privacy' (2018) 25 University of Maryland Francis King Carey School of Law Legal Studies Research Paper 1870, p. 1882. Available on SSRN: http://ssrn.com/abstract=3233805 (last accessed on 18 April 2020).

victim having any control over it. Most victims of deepfake pornography are female.[71] This is the gendered dimension of deepfake pornography. It strongly shows gender inequality, which is seen as morally impermissible by many.[72]

Besides the aforementioned issues, there are two issues regarding the creator/poster of the non-consensual deepfake pornography. Firstly, it may be difficult to identify the person who created and posted the deepfake. Metadata might be insufficient to identify the actual poster, for example when the IP address is used by different persons. The online world also offers many possibilities for the poster to stay anonymous, such as Tor. Tor is a technology that routes internet traffic through different servers and encrypts this, which makes it very hard to find the source of information or the location of the user.[73] Besides this, the poster of the video might not be the actual creator of the video, which can make it difficult to pinpoint who the actual perpetrator is.[74]

Another issue is caused by the global character of the Internet. The poster may not be within the jurisdiction of the state where the investigation and the judicial process are taking place.[75] There is no harmonisation of rules regarding deepfake technology on an international level yet, so international cooperation may be very difficult in these cases.[76]

When a case is eventually brought to court, there are still some problems. Firstly, civil suits may put a heavy burden on the victim. Civil suits can be time-consuming, costly and emotionally challenging.[77] Furthermore, victims may be reluctant to actually go to court, because they do not desire more unwanted publicity.[78] This is closely linked to the Streisand effect, which describes the situation where the attempt to suppress information makes it more widespread.[79] The harder you try to get something deleted from the Internet, the more you fuel people's interest in it, which defeats the purpose of the intervention.[80] The reason for this is that attention is brought to the subject, and people become curious what all the hassle is about.

---

[71] D. Citron, 'Sexual Privacy' (2018) 25 University of Maryland Francis King Carey School of Law Legal Studies Research Paper 1870, p. 1924. Available on SSRN: http://ssrn.com/abstract=3233805 (last accessed on 18 April 2020); Deeptrace, 'The State of Deepfakes' (2019), p. 4-5. Access online: https://storage.googleapis.com/deeptrace-public/Deeptrace-the-State-of-Deepfakes-2019.pdf (last accessed on 18 April 2020).

[72] C. Öhman, 'Introducting the pervert's dilemma: a contribution to the critique of Deepfake Pornography' (2019) Ethics and Information Technology, p. 5 & 7. Access online: https://rdcu.be/b3DZM (last accessed on 18 April 2020).

[73] Tor Project, https://www.torproject.org/about/history/ (last accessed on 16 April 2020).

[74] B. Chesney & D. Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753, p. 1792.

[75] B. Chesney & D. Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753, p. 1792.

[76] K. Farish, 'Do deepfakes pose a golden opportunity? Considering whether English law should adopt California's publicity right in the age of deepfake' (2020) 15 Journal of Intellectual Property Law & Practice 40, p. 48.

[77] M.A. Franks, 'Criminalizing Revenge Porn: Frequently Asked Questions' (2013), p. 2. Available on SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2337998 (last accessed on 18 April 2020).

[78] D. Citron, 'Sexual Privacy' (2018) 25 University of Maryland Francis King Carey School of Law Legal Studies Research Paper 1870, p. 1930. Available on SSRN: http://ssrn.com/abstract=3233805 (last accessed on 18 April 2020).

[79] K. Farish, 'Do deepfakes pose a golden opportunity? Considering whether English law should adopt California's publicity right in the age of deepfake' (2020) 15 Journal of Intellectual Property Law & Practice 40, p. 48.

[80] D. Stewart & K. Bunton, 'Practical Transparency: How Journalists Should Handle Digital Shaming and "The Streisand Effect"' (2016) 5 Journal of Media Law & Ethics 4, p.4.

2.9 Responding to deepfake technology

Deepfake technology can cause different harms. However, it would be inappropriate to completely ban the technology, as this is deemed unethical.[81] If deepfake technology were to be completely prohibited, the freedom of speech of persons would be limited, because deepfake technology provides a manner in which persons can express themselves. Deepfakes can cause harm in certain contexts, but deepfake technology also creates many benefits, as discussed in section 2.6. These beneficial uses should not be suppressed because of the possible harmful uses of this technology.[82]

Instead, existing legislation should be used to deal with the harmful uses of deepfake technology. If the existing legislation is insufficient, new legislation should be created with a specific focus on harmful uses of deepfake technology. Because there are many different harms concerning a broad array of subjects, this research only focuses on one of the harms caused by deepfake technology. The focus in this research lays specifically on the use of deepfake technology for the creation of non-consensual pornography, because this use creates different specific issues, such as reputational damage due to the stigma on sexual images, infringement of one's (sexual) privacy and the difficulty to take steps against the perpetrator. In the following chapters, current Dutch legislation will be applied to the case of non-consensual deepfake pornography, in order to research whether this legislation can be used in these cases.

[81] M. Westerlund, 'The Emergence of Deepfake Technology: A Review' (2019) 9 Technology Innovation Management Review 39, p. 44.
[82] B. Chesney & D. Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753, p. 1788-1789.

Chapter 3: Criminal law responses

3.1 Introduction

The Dutch Criminal Code (*Wetboek van Strafrecht*, further referred to as 'DCC') contains different provisions that may be applicable to non-consensual deepfake pornography, which will be discussed in this chapter. An explanation of how I came to pick the provisions discussed in this chapter and the next one can be found in section 1.6.

Firstly, article 139h DCC on revenge pornography may be interpreted as to include non-consensual deepfake pornography within its scope. This will be discussed in section 3.2. Furthermore, article 240b DCC on child pornography also includes virtual child pornography. Deepfake pornography can also be regarded to be virtual pornography, so it may also fall within the scope of article 240b DCC. This will be further examined in section 3.3.

Other relevant offences will be discussed in section 3.4, such as insult, defamation and menace. These focus mostly on how the perpetrator acts and what uses are made of the images of the victims. These provisions do not criminalize a certain behaviour because the image is prejudicial in itself, as is the case with revenge pornography and child pornography. These provisions will only be shortly reviewed, because the applicability of the provisions is dependent on the specific circumstances of a case. Instead, there will be a discussion what these crimes entail and how they could possibly be applied to cases of non-consensual deepfake pornography.

In section 3.5 the possibilities for notice and takedown will be discussed, which are of importance for the legal redress that a victim can receive from the provisions that are discussed in sections 3.2 to 3.4.

When discussing the legislation, firstly the intentions of the legislator when creating the law will be examined. After this, there will be an analysis of whether non-consensual deepfake pornography falls under the scope of the provision that is applied. Lastly, the legal redress that the victims can receive under these provisions will be discussed. After discussing these three subjects, a conclusion can be made whether or not the provisions can be used in the case of non-consensual deepfake pornography.

3.2 Revenge pornography

The Dutch Criminal Code contains a provision that criminalizes revenge pornography: article 139h DCC.[83] This article was introduced by the Dutch legislator in 2019. There was an increase in the misuse of sexual imagery in order to bring the portrayed person in a negative light.[84] According to the parliamentary history on article 139h DCC, the legislator sees this as an infringement of a person's (sexual) privacy.[85] Because sexual imagery is very sensitive and intimate material, the portrayed person should have agency over the creation and publication of the imagery. In cases of revenge pornography, this is not the case, which creates an infringement of the privacy of the portrayed person.[86] For this reason, and because revenge pornography can deeply negatively affect the lives of the victims, the legislator was of the opinion that revenge pornography needed to be criminalized.[87]

[83] See Annex I for the Dutch text and English translation of article 139h of the Dutch Criminal Code.
[84] *Kamerstukken II*, 2018/19, 35080, 3, p. 3-4.
[85] *Kamerstukken II*, 2018/19, 35080, 3, p. 4.
[86] *Kamerstukken II*, 2018/19, 35080, 3, p. 4.
[87] *Kamerstukken II*, 2018/19, 35080, 3, p. 4.

Before the introduction of this law, the creation and publication of revenge pornography was already penalized under provisions regarding insult and crimes against personal freedom, which will be reviewed in section 3.4. These provisions are a lex generalis, while article 139h DCC is a lex specialis. The legislator was of the opinion that a more specific criminal provision was necessary for revenge pornography. The reason for this is that the provisions regarding insult and crimes against personal freedom do not cover the implications that revenge pornography has on the society and the victims, because the focus of those provisions is on how the perpetrator uses the images, and not on the fact that the image is harmful in itself. Having a specific criminal provision on revenge pornography gives victims recognition for the harm that has been done to them with revenge pornography. It shows that the non-consensual creation and/or use of the sexual image is bad in itself, and does not impose a sanction depending on what the perpetrator does with the pictures, such as is the case with the provisions regarding insult and crimes against personal freedom. Furthermore, it gives a strong signal to (potential) perpetrators that this behaviour is not to be tolerated.[88]

Article 139h DCC focuses on three kinds of behaviour relating to non-consensual pornography. Firstly, the deliberate creation of a sexual image of a person without the knowledge or consent of the portrayed person is criminalized in article 139h(1)(a) DCC. Furthermore, article 139h(1)(b) DCC criminalizes the possession of such a sexual image, when the holder of these images knew or reasonably should have known that that image was created deliberately and without the knowledge or consent of the portrayed person.[89] Lastly, article 139h(2) DCC focuses on the disclosure and publication of revenge pornography. Article 139h(2)(a) DCC criminalizes the publishing of an image that is created in a deliberate and unlawful manner, such as described in article 139h(1)(a) DCC. Article 139h(2)(b) DCC penalizes the publishing of a sexual image of a person, while the person who published the image was aware that the publishing could be harmful for the portrayed person.

A sexual image is defined in the explanatory report as an image of such an intimate sexual character that any reasonable person would consider the image to be private.[90] An image is understood as any kind of image, such as photographs, videos or images of a livestream.[91] The term ‘creation’ (*vervaardigen*) is not defined in the provision or the commentary to the provision, so doubts still arise with regard to the exact meaning of this term. It could be interpreted as being limited to taking a picture, but it could also be broader, for example covering the creation of sexual images in Photoshop as well. Because the legislator also wants to cover new and future types of publishing sexual images, I assume that the term ‘creation’ should be interpreted broadly.[92]

The provision applies to non-consensual pornography and the non-consensual publishing of sexual images. The question arises whether non-consensual *deepfake* pornography also falls under the scope of article 139h DCC. Because there is no case law with regard to this provision yet, it is difficult to pinpoint whether it is necessary to prove that the

[88] *Kamerstukken II*, 2018/19, 35080, 3, p. 4.
[89] *Kamerstukken II*, 2018/19, 35080, 3, p. 4-5.
[90] J.M. ten Voorde, ‘Vervaardigen enz. van afbeelding van seksuele aard’ (2020) T&C Strafrecht, commentaar op art. 139h Sr. Access online: https://www.navigator.nl/document/idpassec16055901db4dc4a1b1827e3061c72e?ctx=WKNL_CSL_581 (last accessed on 23 May 2020).
[91] *Kamerstukken II*, 2018/19, 35080, 3, p. 22.
[92] *Kamerstukken II*, 2018/19, 35080, 3, p. 5.

pornographic image is real. The legislator has not expressed their views on this explicitly, but does seem to do so implicitly in the explanatory report. The legislator namely states that the scope of criminalization is set up in such a way that new and future types of publishing sexual images with the intent to harm the portrayed person will also fall within the scope.[93] Non-consensual deepfake pornography can be regarded as sexual images, because they are images of an intimate sexual character. The fact that the deepfake images are not real do not take away this characteristic nor the potential damage they can procure to the victims, which is in all similar to that of real images of sexual nature. It can thus be argued that when these deepfakes are created without the consent of the portrayed person or published with the intention to put the portrayed person in a negative light, this behaviour would fall within the scope of article 139h DCC.

When this provision was proposed, there was criticism by the legal scholar Goudsmit that it focuses on the intention of the perpetrator, instead of on the harm done to the victim.[94] This focus on the intention of the perpetrator is problematic for two reasons. Firstly, the intention of the perpetrator may be very difficult to prove, especially in cases where the image is published online without any comment alongside it that show his or her intention.[95] This renders the provision practically useless, because it is very difficult to have strong proof of the actual intention of the perpetrator. Because there have been no court cases yet where this provision has been used, it cannot be researched yet how public prosecutors and the court actually deal with this requirement.

The second reason why the focus on the intention of the perpetrator is problematic is that this requirement disregards the wrongs done to the victim. The harm that has been done to the victim is not dependent on the intention of the perpetrator, it is dependent on the fact that their sexual image is created and/or published without their knowledge and/or consent.[96] However, the legislator has fully focussed on the intention of the perpetrator instead of the harm done to the victim. This creates a risk that there will be cases that fall outside the scope of this provision, even when significant harm has been done to the victim.

When it is proven that the perpetrator created or possessed a sexual image intentionally and without the knowledge or the consent of the portrayed person, the perpetrator can be imprisoned for a maximum of one year or receive a fine of the fourth category.[97] A fine of the fourth category could maximally be a fine of €21.750. If the perpetrator has published a sexual image as described in article 139h(1)(a) DCC or has published a sexual image while knowing that this could be harmful for the portrayed person, the perpetrator can be sentenced to a maximum of two years imprisonment or receive a fine of the fourth category.[98]

The conclusion can be made that it is very likely that non-consensual deepfake pornography falls within the scope of article 139h DCC. However, the requirement to prove the intention of the perpetrator might make it difficult to actually use this provision to

[93] *Kamerstukken II*, 2018/19, 35080, 3, p. 5.
[94] M. Goudsmit, 'Criminalising Image-based Sexual Abuse: an Analysis of the Dutch Bill against Revenge Pornography' (2019) 68 Ars Aequi 442, p. 445.
[95] M. Goudsmit, 'Criminalising Image-based Sexual Abuse: an Analysis of the Dutch Bill against Revenge Pornography' (2019) 68 Ars Aequi 442, p. 445-446.
[96] M. Goudsmit, 'De wijzende vinger bekeken: over de strafbaarstelling van wraakpornografie' (2018) 24 NJB 1721, p. 1726.
[97] Article 139h(1) DCC.
[98] Article 139h(2) DCC.

prosecute a perpetrator. For this reason, other options within criminal law will be discussed in the following sections.

3.3 Child pornography

If a minor is portrayed in non-consensual deepfake pornography, article 240b DCC on child pornography may be applicable.[99] The provision penalizes the production, distribution, public offering or possession of images that show a minor engaged in a sexual act. A minor is a person below the age of 18.[100] In 2002, virtual child pornography was included as a punishable offence under article 240b DCC. This was done by adding the wording "seemingly involving" (*waarbij (…) schijnbaar is betrokken*) to the text of article 240b DCC. Virtual child pornography is any kind of image where a child is seemingly involved in a sexual act. This kind of child pornography can be created through the use of images of real children or persons, or through the use of completely virtual images.[101]

The legislator had different reasons to include virtual child pornography as a punishable offence. The first reason to criminalize virtual child pornography was further protection of children. Article 240b DCC criminalizes child pornography in order to protect children from sexual abuse. By adding virtual child pornography to this article, it would also prevent damage created by publishing footage that suggests the sexual abuse of children.[102] It protects against behaviour that is used to encourage children to engage in sexual behaviour and become part of a subculture that promotes the sexual abuse of children.[103]

A second reason to include virtual child pornography in article 240b DCC is that this makes it easier to prosecute someone for committing this offence. It is not necessary anymore to prove that a real child was involved to the creation of the sexual image.[104] This makes it easier for the public prosecutor to prove that there is a case of child pornography as is criminalized in article 240b DCC. It used to be very difficult to prove this on the basis of the footage, because virtual child pornography can be indiscernible from real child pornography.[105]

Lastly, the legislator followed the international consensus.[106] This international consensus becomes clear when looking at article 9(2) of the Cybercrime Convention, which is the first international treaty that addresses cybercrime and has currently been ratified by 65 states.[107] This article clarifies what is understood to be child pornography. "Realistic images representing a minor engaged in sexually explicit conduct" is mentioned in sub c of this article.[108] Virtual child pornography thus also falls within the scope of this article of the Cybercrime Convention, and it becomes clear that it is mandatory for the parties of the Cybercrime Convention to criminalize this type of child pornography in national legislation as well. This is what the Dutch legislator has done in article 240b DCC.

---

[99] See Annex II for the Dutch text and English translation of article 240b of the Dutch Criminal Code.
[100] S. van der Hof, 'Wraakporno op Internet' (2016) 65 Ars Aequi 54, p. 55.
[101] *Kamerstukken I*, 2001/02, 27745 (memorie van antwoord), p. 7.
[102] *Kamerstukken II*, 2000/01, 27745, 3, p. 4.
[103] *Kamerstukken I*, 2001/02, 27745, 299b, p. 1 and 3.
[104] *Kamerstukken II*, 2000/01, 27745, 3, p. 5.
[105] *Kamerstukken I*, 2001/02, 27745, 299b, p. 3.
[106] *Kamerstukken II*, 2000/01, 27745, 3, p. 4; *Kamerstukken I*, 2001/02, 27745, 299b, p. 7.
[107] Council of Europe, 'Chart of signatures and ratifications of Treaty 185 – Convention on Cybercrime'. Access online: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=RnKq5xsu (last accessed on 17 April 2020).
[108] Article 9(2)(c) Cybercrime Convention.

Article 240b DCC covers three different kinds of child pornography: a sexual image of a real child, a sexual image of a real person who looks like a child, and a realistic sexual image of a non-existing child.[109] In the discussion regarding deepfake pornography, only the last type of child pornography is of importance, the realistic image of a non-existing child. No real child or person posing to be a child is involved in the sexual deepfake, which is why only virtual pornography is of importance.

A recurring objection against penalizing virtual child pornography was that this criminalisation would be too broad and could infringe on the fundamental rights to privacy and the freedom of expression, for example because someone could not make a drawing of a naked child anymore, as this might fall within the scope of the legislation.[110] The legislator protected these rights by only criminalizing virtual child pornography that is undiscernible from reality. This is similar to the Cybercrime Convention, which also only criminalizes realistic images.[111] Paintings, drawings, comics and cartoons do not fall within the scope of article 240b DCC.[112] In this manner, people still have the freedom for creative expressions.

The limitation of the scope to virtual child pornography that is undistinguishable from real child pornography also becomes clear from Dutch case law. A judgement from 2013 by the Dutch High Court is of importance here.[113] In this case, the Dutch Public Prosecution Office appealed to the High Court after judgements of the District Court and the Court of Appeal that different drawings of children engaged in sexual acts were not deemed to be child pornography as described in article 240b DCC, because the drawings were not realistic images.[114] In the appeal to the High Court, the public prosecutor argued that these drawings should be deemed to be child pornography in order to protect children against sexual abuse, because these drawings could be used for grooming. According to the public prosecutor, only purely creative and artistic images should be excluded from the scope of article 240b DCC.[115] After reviewing international legislation and the intention of the legislator when adding virtual child pornography to the scope of article 240b DCC, the High Court rejected the appeal. It followed the judgements of the District Court and the Court of Appeal by stating that virtual child pornography only encompasses realistic images of a child engaged in sexual conduct.[116] In a later case where virtual child pornography was discussed as well, the High Court again referred to its judgement from 2013.[117] This rule of realism thus seems to be the standard rule with regard to virtual child pornography.

Deepfake pornography can be deemed to fall within the scope of article 240b DCC, because in most cases it is undiscernible from a real image. The conclusion can be made that when a person below the age of 18 is portrayed in non-consensual deepfake pornography, article 240b DCC can be used when prosecuting the perpetrator. Article 240b DCC can thus be used in cases of non-consensual deepfake pornography where the portrayed person is (deemed to be) a minor.

When it is proven that a person has produced, distributed, publicly offered or possessed (virtual) child pornography, the perpetrator can be sentenced to imprisonment for a

[109] *Kamerstukken II*, 2001/02, 27745, 6, p. 8.
[110] *Kamerstukken I*, 2001/02, 27745, 299b, p. 6.
[111] Article 9(2)(c) Cybercrime Convention.
[112] *Kamerstukken II*, 2001/02, 27745, 6, p. 14.
[113] HR 12 March 2013, ECLI:NL:HR:2013:BY9719.
[114] HR 12 March 2013, ECLI:NL:HR:2013:BY9719, para. 2.2.2.
[115] HR 12 March 2013, ECLI:NL:HR:2013:BY9719, para. 2.2.2.
[116] HR 12 March 2013, ECLI:NL:HR:2013:BY9719, para. 2.4-2.7.
[117] HR 24 June 2014, ECLI:NL:HR:2014:1497, para. 3.2.2.

maximum of four years or be given a fine of the fifth category.[118] A fine of the fifth category could maximally be a fine of €87.000. Furthermore, if one or more of the acts described in article 240b(1) DCC is done on a professional or habitual basis, the perpetrator can be imprisoned for a maximum of eight years of be given a fine of the fifth category.[119]

Child pornography cases are often cross-border cases. However, prosecution in the Netherlands can still take place in different cases with a cross-border characteristic. A perpetrator can be prosecuted in the Netherlands when the unlawful act takes place in the Netherlands. Furthermore, if child pornography is published on the Internet outside the Dutch jurisdiction but is mostly focussed on the Dutch user market, the perpetrator can be prosecuted in the Netherlands as well. Lastly, if an unlawful act with regard to child pornography takes place outside the Netherlands, but the perpetrator is a Dutch citizen, the Netherlands has jurisdiction in these cases as well.[120]

3.4 Provisions regarding insult and crimes against personal freedom

It is possible to use the provisions of the DCC regarding insult and crimes against personal freedom when dealing with a case of non-consensual deepfake pornography. This section discusses the provisions that criminalize insult[121], defamation[122], aggravated defamation[123], coercion[124], menace[125] and besetting[126]. Which provision is applicable depends on the circumstances of the case.

When sexual images are published on the Internet without the consent of the portrayed person, it can be an insult crime.[127] Depending on the severity of the insult, the perpetrator can be prosecuted on the basis of insult, defamation or aggravated defamation. When someone's honour or good name intentionally gets attacked, this behaviour is deemed to be insult.[128] In cases of defamation, someone's honour or good name gets intentionally attacked by making public that the person has committed a certain act.[129] When these comments that a person committed a certain act are not true, it is a case of aggravated defamation.[130]

In cases of revenge pornography published online, it is important to find out in which context the footage is placed online and what the character of the footage is, specifically in what manner the footage portrays the person.[131] If the non-consensual deepfake pornography

---

[118] Article 240b(1) DCC.
[119] Article 240b(1) DCC.
[120] *Kamerstukken II*, 2001/02, 27745, 6, p. 14-15.
[121] Article 266 DCC. See Annex III for the Dutch text and English translation of article 266 of the Dutch Criminal Code.
[122] Article 261(1 and 2) DCC. See Annex IV for the Dutch text and English translation of article 261 of the Dutch Criminal Code.
[123] Article 262 DCC. See Annex V for the Dutch text and English translation of article 262 of the Dutch Criminal Code.
[124] Article 284 DCC. See Annex VI for the Dutch text and English translation of article 284 of the Dutch Criminal Code.
[125] Article 285 DCC. See Annex VII for the Dutch text and English translation of article 285 of the Dutch Criminal Code.
[126] Article 285b DCC. See Annex VIII for the Dutch text and English translation of article 285b of the Dutch Criminal Code.
[127] S. van der Hof, 'Wraakporno op Internet' (2016) 65 Ars Aequi 54, p. 56.
[128] Article 266 DCC; S. van der Hof, 'Wraakporno op Internet' (2016) 65 Ars Aequi 54, p. 56.
[129] Article 261 (1 and 2) DCC; Hof Amsterdam 19 October 2017, ECLI:NL:GHAMS:2017:4648; Hof Den Haag 13 June 2018, ECLI:NL:GHDHA:2018:2017.
[130] Article 262 DCC; S. van der Hof, 'Wraakporno op Internet' (2016) 65 Ars Aequi 54, p. 56.
[131] Hof Leeuwarden 4 May 2010, ECLI:NL:GHLEE:2010:BM3169.

is placed online with the intention to attack someone's honour or good name, the perpetrator could be prosecuted on the basis of insult. If it brings across the message that someone has committed a certain act, it is a case of defamation. A deepfake can be deemed to be a defamatory. In case that the statement or image is fake, it is a case of aggravated defamation. A perpetrator who published non-consensual deepfake pornography in order to attack someone's honour or good name may likely be prosecuted on the basis of aggravated defamation. The non-consensual deepfake pornography portrays an act that the portrayed person has never committed, and for this reason the message it brings across that someone committed a certain act is not true. Depending on which type of insult crime is proved at the court, a perpetrator can be prosecuted to maximally two years in prison or be given a fine of the fourth category.

Besides attacking someone's honour or good name, the sexual image can also be used to pressure someone into doing certain things, such as paying money in order not to have the footage published online.[132] Depending on the concrete situation, this can lead to cases of coercion, menace or besetting. In case of coercion, the perpetrator threatens to commit defamation if a person does not do something that the perpetrator wants them to do.[133] If non-consensual deepfake pornography is used in this manner, the perpetrator can thus be prosecuted on the basis of coercion. When the perpetrator threatens to publish the sexual image in order to attack someone's honour or good name, this is a case of menace.[134] When a perpetrator systematically and intentionally infringes someone's private life in order to force them to commit certain acts or be withheld to do something, this is a case of besetting.[135] In the context of deepfake pornography, I argue that the behaviour takes place systematically when the perpetrator publishes several deepfakes or repeatedly posts the footage online. The perpetrator can be prosecuted to a maximum of four years of imprisonment or receive a fine of the fourth category.

Before the implementation of article 139h DCC, the aforementioned provisions were used in cases regarding revenge pornography. In these cases, the courts saw the publication of sexual images on the Internet as a completely unacceptable act. The court stated in its legal decision of 13 June 2018 that the publication of revenge pornography is completely unacceptable, due to the impact that this has on the victim.[136] The sexual image is very difficult to remove from the internet, and may remain online forever. Furthermore, it has a big effect on the life of the victim, because it significantly infringes their privacy.[137] Even though the courts saw it as a completely unacceptable act, the low sanctions were given, mostly consisting out of community service.[138]

The provisions discussed in this section can be used in cases of non-consensual deepfake pornography. This may be very useful when it is difficult to prove that the publication of non-consensual deepfake pornography falls within the scope of article 139h DCC. Because these articles mostly focus on what the perpetrator does with the sexual images, for example threaten someone or insult someone, instead of giving out the message

[132] S. van der Hof, 'Wraakporno op Internet' (2016) 65 Ars Aequi 54, p. 57.
[133] Article 284 DCC.
[134] Article 285 DCC.
[135] Art 285b DCC.
[136] Hof Den Haag 13 June 2018, ECLI:NL:GHDHA:2018:2017.
[137] Hof Den Haag 13 June 2018, ECLI:NL:GHDHA:2018:2017; Rb. Gelderland 30 March 2018, ECLI:NL:RBGEL:2018:1461; Rb. Leeuwarden 9 April 2009, ECLI:NL:GHLEE:2010:BM3169.
[138] Hof Den Haag 13 June 2018, ECLI:NL:GHDHA:2018:2017; Rb. Gelderland 30 March 2018, ECLI:NL:RBGEL:2018:1461; Rb. Leeuwarden 9 April 2009, ECLI:NL:GHLEE:2010:BM3169.

that the non-consensual creation or publication of sexual images is not allowed, it seems more desirable to use article 139h DCC first, and secondarily focus on the provisions regarding insult and crimes against personal freedom. Furthermore, the use of article 139h DCC may lead to higher sanctions than the use of the standard criminal legislation. However, it is important to note that this cannot be said with certainty, because there is no case law yet where article 139h DCC is used.

3.5 Notice and takedown

The conviction of the perpetrator does not take away the harm that has been done to the victim. When the sexual image is placed online, it will still be there after the perpetrator gets sentenced, where it can be accessed and shared further. The legislator is aware of this, and has expressed that it is important that the sexual images can be deleted from the Internet as soon as possible.[139] There are different possibilities to remove the sexual image from the Internet.

Firstly, a request can be made to delete the image at the platform where the image has been posted. Big social media platforms, such as YouTube and Instagram, have a policy for deleting images that are against the rules of the platform. The publication of non-consensual pornography is against the rules of most platforms, so it is very likely that these images will be deleted upon request. Furthermore, a European code of conduct exists between the EU and big social media companies that emphasizes the importance of complying with European legislation. It obligates the social media platforms to respond to deletion-requests within 24 hours of receiving that request.[140]

Furthermore, the code of conduct Notice and Takedown was set up in the Netherlands in 2008. It contains a procedure for intermediaries, such as Internet Service Providers, on how they should handle requests to delete unlawful content on the Internet. Any person can report unlawful content to the intermediaries, who will have to review the content and delete it when it is deemed unlawful. If the content is not deleted, the person who has reported it can declare a criminal offence.[141] This forces intermediaries to delete unlawful content, such as non-consensual pornography, from the Internet.

Lastly, the public prosecutor has the power to order the deletion of criminal content from the Internet in order to stop criminal offences or to make sure that no new criminal offences take place. This power of the public prosecutor is laid down in article 125p of the Dutch Code of Criminal Procedure.[142]

These possibilities may be useful when requesting the deletion of non-consensual deepfake pornography from the Internet. However, content can spread very quickly on the Internet through sharing, downloading and placing the content on other websites. It can thus be very difficult to fully delete the content from the Internet, because there might always be a chance that it appears again.[143]

---

[139] *Kamerstukken II*, 2018/19, 25080, 3, p. 12.
[140] *Kamerstukken II*, 2018/19, 35080, 3, p. 12-13.
[141] *Kamerstukken II*, 2018/10, 35080, 3, p. 13.
[142] Article 125p of the Dutch Code of Criminal Procedure. See Annex IX for the Dutch text and English translation of article 125p of the Dutch Code of Criminal Procedure.
[143] D. Harris, 'Deepfakes: False Pornography is Here and the Law cannot Protect You' (2019) 17 Duke Law & Technology Review 99, p. 119.

3.6 Conclusion

There are different provisions of the DCC that can be used when dealing with non-consensual deepfake pornography. The different provisions have their own advantages and disadvantages.

There is no clarity yet whether the provision against revenge pornography[144] also covers non-consensual deepfake pornography. There has not yet been any case law with regard to this, so it is unsure whether the court will actually prosecute perpetrators on the basis of this provision in cases of non-consensual deepfake pornography. It may be desirable to explicitly mention virtual pornography in the provision, which has been done in the provision against child pornography as well.

The provision against child pornography[145] is very useful when dealing with non-consensual deepfake pornography, because the article explicitly mentions virtual pornography. Non-consensual deepfake pornography thus falls within the scope of this provision. However, this can only be used for footage of minors. It will not provide any legal redress for people above the age of 18 who are portrayed in a deepfake.

Provisions regarding insult and crimes against personal freedom are very dependent on the specific situation of the case. The focus is mostly on what the perpetrator does, instead of giving out the message that for example creating and/or sharing revenge pornography is an unacceptable act. Furthermore, case law shows that revenge pornography cases where these provisions are used lead to low sanctions for the perpetrator, which is undesirable. It may be better to use the aforementioned specific provisions on revenge pornography and child pornography.

[144] Article 139h DCC.
[145] Article 240b DCC.

Chapter 4: Responses from other branches of the law

4.1 Introduction

After the discussion on the possible application of Dutch criminal law in chapter 3, this chapter will examine two more pieces of legislation. Firstly, the portrait right will be discussed in section 4.2. After this, the right to be forgotten will be applied to the case of non-consensual deepfake pornography in section 4.3.

4.2 Portrait right

The portrait right (*portretrecht*) is part of Dutch copyright law. The relating provisions can be found in articles 19 to 21 of the Dutch Copyright Law (*Auteurswet*, further referred to as 'DCL')[146].

The portrait right is strongly connected to the right to protection of personal life of article 8 of the European Convention of Human Rights (further referred to as 'ECHR'). This becomes clear from a case decided by the European Court of Human Rights in 2009. The Court states that the notion of private life in article 8 ECHR is a broad concept, which also encompasses the right to identity and the right to personal development.[147] With regard to a person's image, the Court states that "*a person's image constitutes one of the chief attributes of his or her personality, as it reveals the person's unique characteristics and distinguishes the person from his or her peers.*"[148] For this reason, the protection of one's image is deemed essential for someone's identity and personal development. The Court concludes that a person should have the right to control the use of his or her image.[149] The portrait right protects someone's right to identity and personal development, and is thus strongly linked to article 8 ECHR.

In Dutch law, a distinction can be made whether a portrait is made by order or not. When a portrait is made by order, the consent of the portrayed person or his/her relatives is needed when publishing the portrait.[150] This is regulated by articles 19 and 20 DCL. When a portrait is not made by order, the image can be published without the permission of the portrayed person or his/her relatives, unless there is a reasonable interest of these persons not to have the image published.[151] Article 21 DCL covers the situations where a portrait is not made by order.

Deepfake pornography portrays a person and can thus be seen as a portrait. This means that the portrait right could apply in cases of non-consensual deepfake pornography. Because the non-consensual deepfake pornography is by definition not created by order of the person who is portrayed in the deepfake, the focus will be on article 21 DCL. This article states that the creator of a portrait usually can publish the image without the permission of the portrayed person or his/her relatives. However, if there is a reasonable interest to not have the image published, the creator is not allowed to publish the image.[152]

---

[146] See Annex X-XII for the Dutch text and the English translation of articles 19 to 21 of the Dutch Copyright Law.
[147] ECHR 15 January 2009, case 1234/05 (Reklos and Davourlis v. Greece), para. 39.
[148] ECHR 15 January 2009, case 1234/05 (Reklos and Davourlis v. Greece), para. 40.
[149] ECHR 15 January 2009, case 1234/05 (Reklos and Davourlis v. Greece), para. 40.
[150] Article 19 and 20 DCL.
[151] Article 21 DCL.
[152] Article 21 DCL.

In the case of non-consensual deepfake pornography, the publication of sensitive materials and materials that are not true but can be mistaken to be true, which can damage the public image of an individual, seem like strong reasonable interests against the publication of the image. This can be illustrated with a case from the Dutch High Court from 1988, where a picture was published of a woman who was intimately holding a man while walking in a park.[153] It did not regard a picture of a sensitive nature, but a picture that was deemed to be intimate. The Dutch High Court stated that when the publication of an image infringes on someone's right to protection of personal life of article 8 ECHR, this can be seen as a reasonable interest of the portrayed person to not have the image published.[154] Non-consensual deepfake pornography strongly infringes on someone's right to protection of personal life, even if it is a fake image, because it shows something sexual, which is deemed to be intimate and personal. Because deepfakes can look very realistic, I argue that it does not matter whether the image is real or not, because it would still come across as something intimate and personal, especially for persons who do not realize that the image is fake. For this reason, the ruling of the High Court in the case from 1988 can apply here as well. This can thus be seen as a reasonable interest not to have the image published. Therefore, it seems that article 21 DCL can be used in cases of non-consensual deepfake pornography.

An argument that can brought forward against using article 21 DCL in cases of deepfakes is that it concerns a doctored image. There is no case law yet whether article 21 DCL covers doctored images as well. However, someone's image is still used, even if it is just partially, so it seems that the argument can be made that it still concerns someone's image and for this reason should still fall within the scope of article 21 DCL.

Article 21 DCL gives the portrayed person the power to prohibit the publication of the image. In cases where the image is still or already published, the portrayed person can ask the creator of the image to stop the publication of the image. The portrayed person can also ask for compensation. Furthermore, an infringement of a right to image is seen as a criminal offence, and the perpetrator can receive a fine of the fourth category.[155]

The portrait right could be used in cases of non-consensual deepfake pornography, but it brings forward several issues as well. An issue that was brought forward in an article focussed on the United States was that the victim itself needs to act and, if necessary, bring the case to court. This may make the victim hesitate, because it can be costly, time consuming and emotionally difficult. It puts an extra burden on the victim that not every victim is able to carry.[156] This issue may also be applicable in the Netherlands. The victim needs to get in contact with the perpetrator, and start a court case if this person does not comply. This can be quite difficult for a victim. This can be illustrated with a Dutch case where a woman became a victim of revenge pornography, and had to search for the sexual image online and start several court cases against the perpetrator.[157] Furthermore, they imply the need to have legal advice or a lawyer, which might be quite expensive. Victims might thus be hesitant to take steps

[153] HR 1 July 1988, NJ 1988/1000.
[154] HR 1 July 1988, NJ 1988/1000, para. 3.3.
[155] Article 35 DCL. See Annex XIII for the Dutch text and English translation of article 35 of the Dutch Copyright Law.
[156] D. Citron, 'Sexual Privacy' (2018) 25 University of Maryland Francis King Carey School of Law Legal Studies Research Paper 1870, p. 1930. Available on SSRN: http://ssrn.com/abstract=3233805 (last accessed on 18 April 2020).
[157] J. Haspels, 'Anne, slachtoffer van wraakporno, ging door hel: "Rechtzaak ter afsluiting"' (28 April 2018) AD. Access online: https://www.ad.nl/den-haag/anne-slachtoffer-van-wraakporno-ging-door-hel-rechtszaak-ter-afsluiting~afb59ccd/?referrer=https://www.google.nl/ (last accessed on 26 April 2020).

under the right to image. When taking steps under criminal law, a public prosecutor will start a case against the perpetrator if there is sufficient evidence, which puts much less pressure on the victim, as they do not have to take these steps by themselves.

Another issue is that it might be difficult for the victim to identify the perpetrator.[158] The reason for this is that the perpetrator can easily stay anonymous, as is explained in section 2.7. Without knowing the identity of the perpetrator, the chances to take effective legal steps against them are very low. Social media websites such as Facebook are not always willing to share information about the perpetrator. A case in the Netherlands where Facebook refused to share the information of a person who published revenge pornography online illustrates this.[159] After two court cases the victim was able to let someone research the Facebook data in order to find out the identity of the perpetrator.[160] This shows that victims have to go through a lot before they are able to properly identify the perpetrator. Because the police have more powers and possibilities to find out the identity of a perpetrator, it might be recommended to report the case at the police and take steps within criminal law instead of taking steps through civil law.

For the reasons discussed above I come to the conclusion that the portrait right can be used in cases of non-consensual deepfake pornography, but that it may be more desirable to take steps under criminal law as this puts less pressure on the victim and gives the ability to use more powers to gather evidence, namely through the powers that the police have.

4.3 GDPR – the right to be forgotten

Article 17 GDPR[161] contains the right to erasure, which is also known as the right to be forgotten. The Dutch translation of article 17 GDPR is laid down in article 17 of the Algemene Verordening Gegevensbescherming (AVG). However, for the sake of clarity and convenience, the right to be forgotten will be discussed referring to article 17 GDPR, because it is the exact same text as the Dutch text and also applicable within Dutch law.

The right to be forgotten was introduced in the Google Spain case[162], where the Court held that an Internet search engine has to consider requests from individuals to remove certain links that show up after searching their name. When information relating to an individual is inaccurate, inadequate, irrelevant or excessive, individuals have the right to request erasure of the personal data. It is not an absolute right, but instead must be balanced with other rights and interests, such as the right of the general public to have access to certain information.[163]

The right to be forgotten developed in the Google Spain case was included in the General Data Protection Regulation of 2018. A data subject has the right to let a controller erase personal data concerning him or her on different grounds, which are laid down in article

---

[158] B. Chesney & D. Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security' (2019) 107 California Law Review 1753, p. 1792.
[159] De Volkskrant, 'Slachtoffer wraakporno heeft recht op gegevens Facebook' (25 June 2020). Access online: https://www.volkskrant.nl/cultuur-media/slachtoffer-wraakporno-heeft-recht-op-gegevens-facebook~bcf82389/ (last accessed on 26 April 2020).
[160] De Volkskrant, 'Slachtoffer en Facebook schikken in wraakpornozaak' (3 March 2016). Access online: https://www.volkskrant.nl/nieuws-achtergrond/slachtoffer-en-facebook-schikken-in-wraakpornozaak~bda81aef/?referer=https%3A%2F%2Fwww.google.nl%2F (last accessed on 26 April 2020).
[161] See Annex XIV for the English text of article 17 of the General Data Protection Regulation.
[162] ECJ 13 May 2014, ECLI:EU:C:2014:317 (Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González).
[163] FRA/ECtHR/EDPS, Handbook on European Data Protection Law (2018), p. 224-225. Access online: https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition (last accessed on 18 April 2020).

17(1) GDPR. A balancing test takes place between the right to privacy and the rights of interested parties and the freedom of expression.[164] This requirement of balancing interests becomes clear from article 17(3)(1) GDPR, where it is stated that the right to erasure does not apply when the processing is necessary for exercising the right of freedom of expression and information.

When applying article 17 GDPR to the case of non-consensual deepfake pornography, it is first important to establish whether these sexual images are personal data. According to article 4(1) GDPR, personal data is any information relating to an identified or identifiable person. Deepfake pornography can be seen as personal data, because it shows the face of a person, and can thus be seen as information that relates to an identified or identifiable person. Furthermore, according to the Dutch legislator, when pictures or videos of persons are shared online, this constitutes the processing of personal data.[165] This means that the portrayed person could request erasure of these sexual images under article 17 GDPR, because it is personal data.

Furthermore, one of the grounds that is mentioned in article 17(1) GDPR has to apply, such as the processing of personal data being unlawful or no longer necessary. In cases of non-consensual deepfake pornography, the ground of article 17(1)(4) GDPR, unlawful processing of personal data, seems to apply. Processing is only lawful when it takes place on one of the grounds mentioned in article 6 GDPR, which is the provision that provides grounds for lawful processing.[166] When non-consensual deepfake pornography is published online by someone who is not the person who is portrayed in the footage, which will often be the case, none of the grounds of article 6 GDPR seem to apply. This will thus lead to the unlawful processing of personal data, and gives the data subject a right to erasure.

Besides the rule that one of the grounds of article 17(1) GDPR has to apply, the right to privacy of the person who requests erasure also has to be balanced against the rights of interested parties and the freedom of expression.[167] Because there is no case law regarding the GDPR and deepfakes or other misrepresentations of someone, only assumptions can be made at the moment of writing. In cases regarding non-consensual deepfake pornography it seems likely that the right to privacy of the portrayed person prevails over the rights to information and freedom of expression. The right to information does not seem to apply with regard to false information. Furthermore, even though the footage is not real, it can be considered to be very intimate and sensitive, and therefore may prevail over the other involved interests.

The controller has the obligation to erase personal data without undue delay when the right to erasure applies. In certain cases, he also has to inform other controllers who process the personal data that this data should be erased.[168]

The right to erasure can thus be used in order to remove non-consensual deepfake pornography from the Internet. However, the portrayed person will have to make requests to

---

[164] European Data Protection Board, 'Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engine cases under the GDPR (part 1)' (2019), p. 10. Access online: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-52019-criteria-right-be-forgotten-search_en (last accessed on 18 April 2020).
[165] Kamerstukken II, 2018/19, 35080, 3, p. 11.
[166] See Annex XV for the English text of article 6 of the General Data Protection Regulation.
[167] European Data Protection Board, 'Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engine cases under the GDPR (part 1)' (2019), p. 10. Access online: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-52019-criteria-right-be-forgotten-search_en (last accessed on 18 April 2020).
[168] Article 17(2) GDPR.

the controller who is processing the data. In cases where the footage is spread online on different websites, the portrayed person will have to request different controllers, which might be difficult to do.[169] In the earlier mentioned Dutch case where a woman became the victim of revenge pornography, she could not request removal from Google through email and had to send a letter to the headquarters of Google in the United States in order to actually arrange it.[170] This case took place before the implementation of the GDPR, so at the moment it may be easier to request removal from Google than this case shows. But even when a controller acts upon an erasure request, the footage may still remain online somewhere else or be published on the Internet again.[171] Furthermore, when using this legislation, one focuses on the controller and not necessarily on the perpetrator. The perpetrator will not be prosecuted and may remain unaware of the impacts that his actions have had. For these reasons, using the right to be forgotten may not be the primary option for the victim to deal with non-consensual deepfake pornography that is published online. It would be sensible to use criminal law, and use the right to be forgotten in combination with this in order to remove the content from the internet.

4.4 Conclusion

There are different provisions of Dutch law that can be used when dealing with non-consensual deepfake pornography. After discussing criminal law in chapter 3, this chapter discussed two other provisions: the portrait right and the right to be forgotten.

The portrait right of articles 19 to 21 DCL can be used in cases of non-consensual deepfake pornography. Because someone's portrait is used in the creation of a deepfake this person may request removal when this deepfake is published online. However, victims will have to act by themselves, which may put quite a burden on them, both emotionally and financially. Furthermore, it may be difficult for the victim to identify the perpetrator. The police have more powers to investigate someone's identity and the criminal behaviour of that person, so it may be better to use criminal law instead of civil law in these cases.

The right to be forgotten of article 17 GDPR could be put to use, but because it focusses on the controller of a website where the deepfake is published rather than on the perpetrator himself, this may not have the desired effect of getting sufficient legal redress against the perpetrator. Furthermore, after removing footage from the Internet, the chance exists that the deepfake still remains online somewhere else or is placed online again at a later moment.

---

[169] R.A. Delfino, 'Pornographic Deepfakes – Revenge Porn's Next Tragic Act – The Case for Federal Criminalization' (2019) 88 Fordham Law Review 887, p. 898-901.

[170] J. Haspels, 'Anne, slachtoffer van wraakporno, ging door hel: "Rechtzaak ter afsluiting"' (28 April 2018) AD. Access online: https://www.ad.nl/den-haag/anne-slachtoffer-van-wraakporno-ging-door-hel-rechtszaak-ter-afsluiting~afb59ccd/?referrer=https://www.google.nl/ (last accessed on 26 April 2020).

[171] D. Citron, 'Sexual Privacy' (2018) 25 University of Maryland Francis King Carey School of Law Legal Studies Research Paper 1870, p. 1955. Available on SSRN: http://ssrn.com/abstract=3233805 (last accessed on 18 April 2020); D. Harris, 'Deepfakes: False Pornography is Here and the Law cannot Protect You' (2019) 17 Duke Law & Technology Review 99, p. 119.

Chapter 5: Future Steps

5.1 Introduction

The manner in which Dutch legislation can be used in cases of non-consensual deepfake pornography has been discussed in chapter 3 and 4. The conclusion can be made that different provisions are of use when dealing with a case of non-consensual deepfake pornography, which shows that the statement made by public prosecutor Lodewijk van Zwieten[172] is correct. The provision on child pornography of article 240b DCC can be used in cases where a person below the age of 18 is portrayed in the deepfake. For persons above the age of 18 who are portrayed in a deepfake, it may be more difficult to find legal redress. The revenge pornography provision could be used, but at this moment it is unclear whether deepfakes fall within the scope of article 139h DCC. Furthermore, article 139h DCC focuses on the intention of the perpetrator, which makes the legislation much more difficult to use, because the intention of the perpetrator may be difficult to prove. Provisions regarding insult and crimes against personal freedom could be put to use as well, but the possibilities of using these provisions fully depend on how the perpetrator uses the deepfake instead of the fact that the non-consensual pornographic deepfake is bad in itself.

There also are legislative options outside criminal law. A victim can make use of the portrait right, but this means that the victim needs to take steps themselves, which may put an extra burden on them. Furthermore, it may be difficult for the victim to actually identify the perpetrator. The right to be forgotten can also be used in cases of non-consensual pornography, but then one is not undertaking steps against the perpetrator, but against the controller of a website where the deepfake is published. The website provider may not always comply with a removal request, and even if he does there is still a risk that the footage can be found somewhere else or will be published online again.

After analysing the aforementioned provisions, I conclude that using criminal legislation in cases of non-consensual deepfake pornography is the most desirable option. It is still possible to claim civil damages during the criminal procedure, use the decision by the court to enforce the portrait right and use the GDPR to obtain erasure from different platforms. Using criminal law will give a clear message to the perpetrator that this type of behaviour is unacceptable. This message comes across less clearly, or maybe even not at all, when a person solely takes steps through the portrait right or the right to be forgotten.

However, there are still some gaps and uncertainties with regard to criminal provisions. It is unclear whether virtual pornography falls within the scope of article 139h DCC regarding non-consensual pornography. Furthermore, it is still unclear how the intention of the perpetrator needs to be proven when using article 139h DCC. Provisions regarding insult and crimes against personal freedom may be applicable as well, but because there is no case law on this yet, it is uncertain how these provisions would actually be applied to cases of non-consensual deepfake pornography. The gaps and uncertainties will need to be filled and clarified through case law or changes in the legislation.

In this chapter future steps to deal with non-consensual deepfake pornography are discussed. In section 5.2 it will be examined whether there is a need for legislation that specifically focuses on non-consensual deepfake pornography. In section 5.3 I will argue that

[172] J. Schellevis, 'Zorgen OM over deepfakes: "Risico op oplichting en afpersing"' (7 September 2019) NOS. Access online: https://nos.nl/artikel/2300688-zorgen-om-over-deepfakes-risico-op-oplichting-en-afpersing.html (last accessed on 18 April 2020).

legislation alone is not enough to deal with non-consensual deepfake pornography, and examine the other actors that can play a role. Lastly, section 5.4 contains the conclusion for this chapter.

5.2 Need for specific legislation?

As mentioned in section 5.1, there are still some gaps and uncertainties in the Dutch legislation that could be put to use in cases of non-consensual deepfake pornography. There are different options to provide more clarity, which will be discussed in this section.

Firstly, more clarity can be provided through case law and parliamentary documents. In this manner, it will be clearer whether non-consensual deepfake pornography falls within the scope of certain pieces of Dutch legislation. This will provide more clarity for victims, who will better understand which steps to take.

Secondly, existing provisions could be amended in order to provide more clarity and fill in the gaps. This seems particularly useful with regard to article 139h DCC. Article 139h DCC on revenge pornography could be amended in a similar manner as article 240b DCC on child pornography, in order for virtual pornography to fall within the scope of that law as well. However, an issue that will remain with regard to article 139h DCC is that the intention of the perpetrator has to be proven, which may be difficult. Future case law will have to show how public prosecutors and courts deal with this requirement.

I am of the opinion that it is not necessary to create a specific provision regarding non-consensual deepfake pornography. The aforementioned amendment of article 139h DCC will create the desired clarity and acknowledge the harm that is being done to victims.

Even though different states and countries have criminalized deepfake pornography, national legislation alone will not be effective in cross-border cases.[173] It is likely that cases of non-consensual deepfake pornography have a cross-border character. When footage is shared on the Internet, this can take place on different platforms within different jurisdictions.[174] National legislation will not be sufficient in this case, because this would only be of use in other jurisdictions to a certain extent. It will not give law enforcement the powers that they would have if the case would take place on a national level. For this reason, it is important that arrangements are made on the international level to harmonize how states deal with non-consensual deepfake pornography and deepfakes in general. This can for example be done by adding the creation and publication of non-consensual deepfake pornography and other types of harmful deepfakes as a crime in the Cybercrime Convention, which could create an incentive to harmonise legislation and powers with regard to this type of deepfake in different states. Currently, 65 states have ratified the Cybercrime Convention,[175] which has caused harmonisation of legislation against cybercrime, for example child pornography and hacking, within these states. No other kinds of pornography can be found in the Cybercrime Convention, which means that non-consensual deepfake pornography of a person over the age of 18 currently does not fall within the scope of the Convention. An addition of harmful

---

[173] M. Westerlund, 'The Emergence of Deepfake Technology: A Review' (2019) 9 Technology Innovation Management Review 39, p. 47.

[174] K. Farish, 'Do deepfakes pose a golden opportunity? Considering whether English law should adopt California's publicity right in the age of deepfake' (2020) 15 Journal of Intellectual Property Law & Practice 40, p. 48.

[175] Council of Europe, 'Chart of signatures and ratifications of Treaty 185 – Convention on Cybercrime'. Access online: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=RnKq5xsu (last accessed on 17 April 2020).

deepfakes to the Convention requires states to harmonize the criminalisation of this issue as well.

5.3 Legislation alone is not enough

Legislation alone will not be sufficient to completely obstruct the creation and spreading of this kind of deepfakes. Through legislation you have the possibility to prosecute the perpetrators and receive compensation for the victims. Furthermore, it gives the ability to remove the footage from the Internet on the basis of notice and takedown. However, the footage may still be saved and shared, and the chance still exists that the footage can be found online in the future and causes further harm to the victim.[176]

Legislation alone is thus not enough to stop non-consensual deepfake pornography from causing harm. Other actors play an important role as well in reducing these harms. These actors are the creators of deepfake detection technology, social media companies and society in general. Furthermore, it is important to support victims, which will also be discussed in this section.

5.3.1 Technology

Besides providing the ability to create deepfakes, technology might also provide the possibility to detect deepfakes. Currently it is still possible for humans to spot a deepfake because of small mistakes, such as the lack of blinking or inconsistencies between speech and mouth movements.[177] However, as this technology is further developed and delivers footage that is of an increasingly better quality, it becomes more and more difficult to actually notice that certain media is fake.[178] For this reason it is important to create and use a detection technology that is able to notice these deepfakes, even when they are indiscernible from reality to the naked eye. Furthermore, the detection technology has to keep up with these innovations in deepfake technology.[179] Once a detection technology is created, this technology should constantly be trained and revised so that it will not be outpaced by the developments of deepfake technology.[180]

Because deepfake technology is still quite a new technology, there are only a few projects that focus on the detection of these deepfakes.[181] An example of a deepfake detection technology is the technology used by Gfycat. This website uses an AI that can detect whether a video is fake by comparing it with the original content of the video.[182] Furthermore, in September 2019 Facebook and Microsoft launched the Deepfake Detection Challenge, where

---

[176] K. Farish, 'Do deepfakes pose a golden opportunity? Considering whether English law should adopt California's publicity right in the age of deepfake' (2020) 15 Journal of Intellectual Property Law & Practice 40, p. 48.
[177] M. Westerlund, 'The Emergence of Deepfake Technology: A Review' (2019) 9 Technology Innovation Management Review 39, p. 45.
[178] M. Westerlund, 'The Emergence of Deepfake Technology: A Review' (2019) 9 Technology Innovation Management Review 39, p. 45.
[179] R.A. Delfino, 'Pornographic Deepfakes – Revenge Porn's Next Tragic Act – The Case for Federal Criminalization' (2019) 88 Fordham Law Review 887, p. 937.
[180] E. Thomas, 'In the battle against deepfakes, AI is being pitted against AI' (25 November 2019) WIRED. Access online: https://www.wired.co.uk/article/deepfakes-ai (last accessed on 25 April 2020).
[181] B. Chesney & D. Citron, 'Deepfakes: A Looming Challenge for Privacy, Democracy and National Security' (2019) 107 California Law Review 1753, p. 1787.
[182] L. Matsakis, 'Artificial Intelligence Is Now Fighting Fake Porn' (14 February 2018) WIRED. Access online: https://www.wired.com/story/gfycat-artificial-intelligence-deepfakes/ (last accessed on 18 April 2020).

people were encouraged to do more research into deepfake detection tools.[183] The challenge has only recently ended and the results are not known yet at the time of writing. Time will tell how these detection technologies will be developed and which ones can be put to use.

5.3.2 Social media

Social media companies should act against non-consensual deepfake pornography, which are often shared through social media platforms. Platforms can take action against this, by prohibiting this in their terms and conditions, and then implementing it in content screening-and-removal policies that are put in place on the basis of good-governance principles.[184] Through these policies certain categories of content can be banned from the platforms. Automated filtering technologies and content moderators remove the prohibited content from the platforms and take further steps against the posters if that is deemed necessary.

Reddit and Pornhub have already banned deepfake pornography, and try to remove deepfake pornography that is posted on their platforms.[185] On Reddit it goes against the rule that it is not allowed to impersonate an individual, and therefore the posts and/or the accounts will be deleted.[186] Facebook has prohibited all kinds of deepfake videos on its platform since January 2020, and will either remove or label manipulated media when it is reported or when content moderators notice that the media is manipulated.[187] Twitter will either label or remove manipulated media from its platform, depending on the manner in which it is shared and whether it is likely to do harm. If the media is shared in a deceptive manner and is likely to do harm, then the media will be deleted from Twitter.[188] Most social media companies have thus announced to remove deepfakes, and more specifically deepfake pornography, from their platforms or label the manipulated media as fake. The future will have to tell whether their efforts to keep manipulated media from their platforms are actually sufficient.

In the effort to keep deepfake pornography from the platforms, it is important that there is cooperation between the automated filtering technologies and the content moderators, persons who check content that has been flagged and remove the content that is against the policy of the social media platforms. The automated filtering technologies, where also technologies can be used that were discussed in section 5.3.1, will notice deepfakes that may not be noticed by moderators, because the footage looks undiscernible from reality. Furthermore, it could provide protection to content moderators, who are exposed to shocking and damaging social media posts and can get traumas because of this.[189] Automated filtering

---

[183] Deepfake Detection Challenge. Access online: https://deepfakedetectionchallenge.ai/ (last accessed on 6 April 2020).
[184] B. Chesney & D. Citron, 'Deepfakes: A Looming Challenge for Privacy, Democracy and National Security' (2019) 107 California Law Review 1753, p. 1817.
[185] M. Westerlund, 'The Emergence of Deepfake Technology: A Review' (2019) 9 Technology Innovation Management Review 39, p. 44.
[186] Reddit, 'Do not impersonate an individual or entity' (date unknown). Access online: https://www.reddithelp.com/en/categories/rules-reporting/account-and-community-restrictions/do-not-impersonate-individual-or (last accessed on 26 April 2020).
[187] Facebook, 'Enforcing Against Manipulated Media' (6 January 2020). Access online: https://about.fb.com/news/2020/01/enforcing-against-manipulated-media/ (last accessed on 6 April 2020).
[188] Twitter, 'Building rules in public: Our approach to synthetic & manipulated media' (4 February 2020). Access online: https://blog.twitter.com/en_us/topics/company/2020/new-approach-to-synthetic-and-manipulated-media.html (last accessed on 7 April 2020).
[189] C. Newton, 'The Trauma Floor: The secret lives of Facebook moderators in America' (25 February 2019) The Verge. Access online: https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona (last accessed on 23 May 2020).

allows them to not having to look at every single post, which may reduce the risk of them getting harmed by it. However, relying exclusively on automated filtering is not an option. There is a risk on false positives and false negatives, namely that certain content does not get deleted even though it is against the content policy or does get deleted even though it is not against the policy, which could lead to censorship. For this reason, it is important that there still is human intervention to check whether removal decisions are correct.[190] Therefore it is very important that humans and technology work together to keep deepfake pornography from social media platforms.

5.3.3 Awareness

Besides technology and social media platforms taking action, it is also important to raise public awareness regarding deepfakes and non-consensual deepfake pornography in particular. The public needs to be educated on the harms of non-consensual deepfake pornography. In this manner, people might be able to better protect themselves because they will be aware that they can possibly fall victim to this and what steps they can take in order to protect themselves. Furthermore, it will make people more aware that not everything they see is real.

Education regarding deepfake technology should take place on various levels. Firstly, the general public should be informed about the fact that images or videos may not always be an accurate representation of what happened.[191] This is not only the case for non-consensual deepfake pornography, but also for other types of deepfakes. This will make people realize that they need to critically assess media that they come across online. This information can be provided on social media websites and through other media.

Furthermore, education programs can take place on schools in order to provide proper information about what harm deepfakes, and more specifically non-consensual deepfake pornography, can do.[192] It will make students more aware of this issue and encourage them to be more careful online. It is especially important to focus on this group of people, because they use social media in great numbers and may not always be aware of the effects that posting certain things online may have for them and for others.

The Dutch government is aware that such education campaigns need to take place in education and for the general public, especially with regard to misinformation.[193] If citizens get more knowledge how technology works, they will be able to critically think about it and understand what the effects of it are in society.[194]

Lastly, law enforcement and the judiciary need to be trained and educated on non-consensual deepfake pornography as well. There should be awareness among these actors about what developments are taking place with regard to non-consensual deepfake

---

[190] B. Chesney & D. Citron, 'Deepfakes: A Looming Challenge for Privacy, Democracy and National Security' (2019) 107 California Law Review 1753, p. 1818.
[191] M. Westerlund, 'The Emergence of Deepfake Technology: A Review' (2019) 9 Technology Innovation Management Review 39, p. 45.
[192] R.A. Delfino, 'Pornographic Deepfakes – Revenge Porn's Next Tragic Act – The Case for Federal Criminalization' (2019) 88 Fordham Law Review 887, p. 933.
[193] K.H. Ollongren, 'Brief inzake desinformatie en beïnvloeding verkiezingen' (2018), p. 6-8. Access online: https://www.rijksoverheid.nl/documenten/kamerstukken/2018/12/13/kamerbrief-over-dreiging-desinformatie-en-beinvloeding-verkiezingen (last accessed on 25 April 2020).
[194] K.H. Ollongren, 'Brief inzake desinformatie en beïnvloeding verkiezingen' (2018), p. 7. Access online: https://www.rijksoverheid.nl/documenten/kamerstukken/2018/12/13/kamerbrief-over-dreiging-desinformatie-en-beinvloeding-verkiezingen (last accessed on 25 April 2020).

pornography and how they should act upon it, for example by teaching them about current practices and possibilities to detect these deepfakes. Because deepfake technology is developing on a fast pace, it is of importance that they are regularly updated on the state of the art and developments with regard to detection and prosecution.[195] This will enable them to deal with cases of non-consensual deepfake pornography more easily, for example by knowing what to look out for when investigating deepfakes and what technologies to use to detect them.

5.3.4 Support for victims

With the regulations regarding notice and takedown, which were discussed in section 3.5, it is easier to remove content from the Internet. However, it is important that persons can take steps themselves as well. This currently can be done through the right to erasure of article 17 GDPR, but it is not always easy to get a request for removal fulfilled, as section 4.3 shows. For this reason, I am of the opinion that clearer rules should be introduced so that people can request removal of harmful information regarding them more easily. The existence and publication of non-consensual deepfake pornography can have a big impact on the victim, and it is undesirable that it is a difficult process to get the deepfake removed from the Internet.

Furthermore, it is important that victims of non-consensual deepfake pornography receive support.[196] Victims may be provided with useful support and insights on how to deal with their current situation through support initiatives. For persons below the age of 26, the Dutch website www.helpwanted.nl offers advice and support for people who have become a victim of online sexual abuse.[197] During my research I did not find support groups or websites for persons above the age of 26 who have become a victim of online sexual abuse. I think it is important that a similar support website as www.helpwanted.nl is set up for these persons as well, because it enables victims to receive advice and support.

5.4 Conclusion

The current legislation in the Netherlands can be used when dealing with cases of non-consensual deepfake pornography. Even though there are still certain gaps in the legislation, these gaps can be filled in through future case law and eventual clarifications from the government. Furthermore, existing provisions can be amended so that it involves non-consensual deepfake pornography more clearly within its scope. It is important that there will be a focus on this kind of deepfakes on an international level, because the Internet gives the crime an international character. This makes it difficult to investigate and prosecute persons who create and share these deepfakes through the use of investigative and judicial powers of one national jurisdiction.

Legislation alone is not enough to completely stop the creation and publication of non-consensual deepfake pornography. For this reason, it is of great importance that other actors are involved as well. It is important that detection technologies will be developed that can point out deepfakes, especially when deepfakes are developing to the point where they are undiscernible from reality. Furthermore, social media companies play a role as well. Because the footage is often placed and shared on these platforms, the companies should have clear

---

[195] R.A. Delfino, 'Pornographic Deepfakes – Revenge Porn's Next Tragic Act – The Case for Federal Criminalization' (2019) 88 Fordham Law Review 887, p. 933-934.
[196] R.A. Delfino, 'Pornographic Deepfakes – Revenge Porn's Next Tragic Act – The Case for Federal Criminalization' (2019) 88 Fordham Law Review 887, p. 934-935.
[197] Helpwanted.nl, https://www.helpwanted.nl/ (last accessed on 14 May 2020).

policies regarding this and also enforce these policies. It is of great importance to create awareness among the public. This can make people to understand that not everything they see online can be believed, and they will be able to protect themselves better against becoming a victim and being portrayed in non-consensual deepfake pornography. If someone does become a victim of non-consensual pornography, it is important that this person can receive support. The victim should be able to easily request removal of the deepfake from the Internet, and therefore clear regulations need to be created with regard to this. Besides this, online support is offered for persons below the age of 26 who have become a victim of online sexual abuse.[198] A similar support possibility needs to be set up for persons above the age of 26, because online sexual abuse, including non-consensual deepfake pornography, can have a big impact on their lives as well. Therefore, it is important that they also receive support and advice.

[198] Helpwanted.nl, https://www.helpwanted.nl/ (last accessed on 14 May 2020).

Chapter 6: Conclusion

6.1 Gap in the literature

Different academic articles discuss deepfake technology and its implications. In these articles it is argued that there are beneficial uses of deepfake technology, but also harmful uses that need to be halted.[199] One of these harmful uses is the use of deepfake technology to create non-consensual deepfake pornography, which can have a big impact on the lives of the victims who are portrayed in these deepfakes.[200]

The existing literature on the regulation of deepfake technology specifically focusses on the United States. Different authors have deemed the legislation within different states and on federal level insufficient.[201] The legislation is deemed insufficient because it is often unclear whether deepfakes, and more specifically non-consensual deepfake pornography falls within the scope of the legislation.[202] The reason for this is that the law does not explicitly mention deepfakes, and there is also no case law yet that clarifies this. There are calls in the United States to create specific legislation to criminalize the creation and publication of non-consensual deepfake pornography.[203]

There has been research in Europe on non-consensual pornography[204], but not much research has been conducted on non-consensual deepfake pornography, even though it is an issue here as well. It is important to research this specific type of non-consensual pornography, because it brings forward different issues than in cases regarding other types of non-consensual pornography, for example that it regards a virtual image and not a real sexual image. Currently there is no academic literature on non-consensual deepfake pornography and possible responses against it in Europe. This is a gap in the literature, which I have aimed to fill with my research.

6.2 Main research question

In order to fill the gap that is created by the lack of European research on non-consensual deepfake technology and to provide a starting point for further research, my thesis aims to answer the following research question:

> *What are the legislative possibilities for the government of the Netherlands to obstruct the use of deepfake technology for the creation of non-consensual pornography?*

---

[199] B. Chesney & D. Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy and National Security' (2019) 107 California Law Review 1753.
[200] R.A. Delfino, 'Pornographic Deepfakes – Revenge Porn's Next Tragic Act – The Case for Federal Criminalization' (2019) 88 Fordham Law Review 887.
[201] D. Harris, 'Deepfakes: False Pornography is Here and the Law cannot Protect You' (2019) 17 Duke Law & Technology Review 99; R.A. Delfino, 'Pornographic Deepfakes – Revenge Porn's Next Tragic Act – The Case for Federal Criminalization' (2019) 88 Fordham Law Review 887.
[202] R.A. Delfino, 'Pornographic Deepfakes – Revenge Porn's Next Tragic Act – The Case for Federal Criminalization' (2019, Forthcoming) 88 Fordham Law Review, p. 19.
[203] D. Harris, 'Deepfakes: False Pornography is Here and the Law cannot Protect You' (2019) 17 Duke Law & Technology Review 99.
[204] M. Goudsmit, 'Criminalising Image-based Sexual Abuse: an Analysis of the Dutch Bill against Revenge Pornography' (2019) 68 Ars Aequi 442; S. van der Hof, 'Wraakporno op Internet' (2016) 65 Ars Aequi 54.

6.3 Findings

My research shows that different Dutch provisions can be applicable in cases of non-consensual deepfake pornography, such as the criminal provisions on revenge pornography[205] and child pornography[206]. It is preferable to use criminal legislation instead of civil legislation, because taking action against a perpetrator through criminal law puts less of a burden on the victim. The victim does not have to take steps in order to identify the perpetrator, collect sufficient evidence and bring this all to court. The police and the public prosecutor, who have more powers to investigate cases, could do that in this situation. Furthermore, using criminal law will give a clear message to the perpetrator that this type of behaviour is unacceptable. This message comes across less clearly, or maybe even not at all, when a person takes steps through civil law.

The legislation offers victims sufficient legal redress, especially through the possibility of notice and takedown. When a person below the age of 18 is portrayed in the deepfake, article 240b DCC can apply as virtual pornography falls within the scope of this provision. However, it is difficult to say how the Dutch legislation will be used in cases of non-consensual deepfake pornography where persons above the age of 18 are portrayed. Pieces of legislation, governmental documents or case law currently do not provide clarity on this yet. It is unclear whether non-consensual deepfake pornography falls within the scope of article 139h DCC on revenge pornography or the standard criminal legislation. Furthermore, even if article 139h DCC covers virtual pornography, it is unclear how the intention of the perpetrator needs to be proven, which seems to be an important requirement in this provision.

For this reason, it is important that case law or governmental documents will be created that provide more clarity on how to deal with cases of non-consensual deepfake pornography. It is especially important that case law clarifies how the requirement of article 139h DCC to prove the intention of the perpetrator has to be fulfilled. Furthermore, case law can show how provisions regarding insult and crimes against personal freedom can be applied in cases of non-consensual deepfake pornography. Besides clarifications through case law, current provisions could be amended in order to involve non-consensual deepfake pornography within the scope of the provision. This is especially important with regard to article 139h DCC on revenge pornography. Article 139h DCC should be amended so that virtual pornography clearly falls within the scope of this article, similarly to the amendment of article 240b DCC on child pornography. I think it is not necessary to create a specific law to criminalize the creation and the publication of non-consensual deepfake pornography.

However, the footage may still show up online. Therefore, it is important to note that legislation alone is not sufficient, other actors have to play a role here as well. These actors are the developers of deepfake detection technologies and social media platforms where these deepfakes are shared. Furthermore, it is important to educate persons that not everything that can be found online is real, even though the image, video or audio recording seems undiscernible from reality. People need to be aware that deepfake technology exists, and know what they can do in order to verify whether footage is real and how they should protect themselves so that they will not become a victim themselves. If someone does become a victim, it is important that they are able to request removal of the deepfake from the Internet. Currently this can be done through the right of erasure of article 17 GDPR, but as many persons still struggle with actually getting the content removed, clear arrangements should be

[205] Article 139h DCC.
[206] Article 240b DCC.

made in order for victims to arrange this more easily. Victims also should be able to receive support. For persons below the age of 26 there already is a support initiative for victims of online sexual abuse[207], but I am of the opinion that similar support initiatives should be set up for persons over the age of 26 as well.

6.4 Implications

My research shows that different Dutch provisions can be used when dealing with cases of non-consensual deepfake pornography. Further clarification will be necessary, either through case law or governmental clarification. Current provisions need to be amended in order for non-consensual deepfake pornography to fall within the scope of the provisions more clearly.

The legislator will need to cooperate with other actors such as technology developers and social media companies in order to obstruct non-consensual deepfake pornography and other types of harmful deepfakes. Legislation alone is not sufficient, so cooperation with other actors is of great importance in order to set up a strong strategy against these harmful deepfakes. Further research is needed regarding the cooperation of these actors in order to obstruct the creation and publication of non-consensual deepfake pornography. It is also important to research whether the other actors, such as developers of detection technologies or social media companies, can be held liable when issues arise with regard to non-consensual deepfake technology. One might even look further than just liability and research how one can create incentives for developers to keep developing the detection technologies and for social media companies to keep these deepfakes off their platforms.

In these cases of non-consensual deepfake pornography it is also of great importance that victims receive support, as these deepfakes can have a big impact on them. Therefore, it is important that further research is conducted regarding the support of victims in these cases. This could even be conducted on a broader level, where one looks at the support of victims of online sexual abuse, including non-consensual (deepfake) pornography.

The Internet is a place where borders are not of importance. Criminal behaviour often takes place over different jurisdictions, so it is important to respond to this on an international level. This is also the case for non-consensual deepfake pornography. It may be created within one jurisdiction, posted online to target someone within another jurisdiction and stored on a server in yet another jurisdiction. This makes investigation and prosecution of the perpetrator quite difficult. Therefore, it is important to harmonise legislation regarding deepfakes, and more specifically non-consensual deepfake pornography, on EU level or global level through for example the Cybercrime Convention. Because my research solely focussed on the Netherlands, the international aspect fell outside the scope of my research, but I am of the opinion that it is important that further research is conducted with regard to this this.

6.5 Final thoughts

Currently, one hears about non-consensual deepfake pornography every once in a while, mostly when a famous person falls victim to it. However, it is important that people realize that “normal” persons like you and I can fall victim to this as well. This is a subject that deserves more attention and stronger responses from legislators and other actors that could play a role in stopping non-consensual deepfake pornography from being created and shared online.

[207] Helpwanted.nl, https://www.helpwanted.nl/ (last accessed on 14 May 2020).

Annex

Annex I – Article 139h Dutch Criminal Code (*Wetboek van Strafrecht*)

Artikel 139h Wetboek van Strafrecht	**Article 139h Dutch Criminal Code**
1 Met gevangenisstraf van ten hoogste een jaar of geldboete van de vierde categorie wordt gestraft: **a** hij die opzettelijk en wederrechtelijk van een persoon een afbeelding van seksuele aard vervaardigt; **b** hij die de beschikking heeft over een afbeelding als bedoeld onder a terwijl hij weet of redelijkerwijs moet vermoeden dat deze door of als gevolg van een onder a strafbaar gestelde handeling is verkregen.	**1** With a maximum of one-year imprisonment or a fine of the fourth category will be punished: **a** the person who intentionally and unlawfully manufactures a sexual image of a person; **b** the person who has an image as described under sub a at his disposal while he knows or reasonably should suspect that this image is obtained through an act that is criminalized in sub a.
2 Met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie wordt gestraft: **a** hij die een afbeelding als bedoeld in het eerste lid, onder a, openbaar maakt terwijl hij weet of redelijkerwijs moet vermoeden dat deze door of als gevolg van een in het eerste lid, onder a, strafbaar gestelde handeling is verkregen. **b** hij die van een persoon een afbeelding van seksuele aard openbaar maakt, terwijl hij weet dat die openbaarmaking nadelig voor die persoon kan zijn.	**2** With a maximum of two years imprisonment or a fine of the fourth category will be punished: **a** the person who publishes an image as described under sub 1a, while he knows or reasonably should suspect that this image is obtained through an act that is criminalized in sub 1a. **b** the person who publishes a sexual image of a person while he is aware that the publication can have a negative effect for that person.

Annex II – Article 240b Dutch Criminal Code (*Wetboek van Strafrecht*)

Artikel 240b Wetboek van Strafrecht	**Article 240b Dutch Criminal Code**
1 Met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie wordt gestraft degene die een afbeelding – of gegevensdrager, bevattende een afbeelding – van een seksuele gedraging, waarbij iemand die kennelijk de leeftijd van achttien jaar nog niet heeft bereikt, is betrokken of schijnbaar is betrokken, verspreidt, aanbiedt, openlijk tentoonstelt, vervaardigt, invoert, doorvoert, uitvoert, verwerft, in bezit heeft of zich door middel van een geautomatiseerd werk of met gebruikmaking van een communicatiedienst de toegang daartoe verschaft.	**1** With a maximum of four years imprisonment or a fine of the fifth category the person will be punished who shares, offers, publicizes, openly displays, manufactures, imports, exports, acquires or owns an image – or a data carrier, containing an image – of a sexual act involving or seemingly involving someone who has not reached the age of eighteen years.
2 Met gevangenisstraf van ten hoogste acht jaren of geldboete van de vijfde categorie	**2** With a maximum of six years imprisonment or a fine of the fifth category

wordt gestraft degene die van het plegen van een van de misdrijven, omschreven in het eerste lid, een beroep of een gewoonte maakt.	the person will be punished who commits the offence described in the first paragraph on a professional or habitual basis.

Annex III – Article 266 Dutch Criminal Code (*Wetboek van Strafrecht*)

Artikel 266 Wetboek van Strafrecht	**Article 266 Dutch Criminal Code**
1 Elke opzettelijke belediging die niet het karakter van smaad of smaadschrift draagt, hetzij in het openbaar mondeling of bij geschrift of afbeelding, hetzij iemand, in zijn tegenwoordigheid mondeling of door feitelijkheden, hetzij door een toegezonden of aangeboden geschrift of afbeelding, aangedaan, wordt, als eenvoudige belediging, gestraft met gevangenisstraf van ten hoogste drie maanden of geldboete van de tweede categorie.	**1** Any insult, which is not of a slanderous or libellous nature, intentionally expressed either in public verbally or in writing or by means of an image, or verbally against a person in his presence or by other acts, or by means of written matter or an image sent or offered, shall constitute simple defamation and shall be punishable by a term of imprisonment not exceeding three months or a fine of the second category.
2 Niet als eenvoudige belediging strafbaar zijn gedragingen die ertoe strekken een oordeel te geven over de behartiging van openbare belangen, en die er niet op zijn gericht ook in ander opzicht of zwaarder te grieven dan uit die strekking voortvloeit.	**2** Acts which are intended to express an opinion about the protection of public interests and which are not at the same time designed to cause any more offence or cause offence in any other way than follows from that intent, shall not be punishable as simple defamation.

Annex IV – Article 261 Dutch Criminal Code (*Wetboek van Strafrecht*)

Artikel 261 Wetboek van Strafrecht	**Article 261 Dutch Criminal Code**
1 Hij die opzettelijk iemands eer of goede naam aanrandt, door telastlegging van een bepaald feit, met het kennelijke doel om daaraan ruchtbaarheid te geven, wordt, als schuldig aan smaad, gestraft met gevangenisstraf van ten hoogste zes maanden of geldboete van de derde categorie.	**1** Any person who, by alleging a particular fact, intentionally injures the honour or reputation of another person, with the evident intention of giving publicity to the allegation, shall be guilty of slander and shall be liable to a term of imprisonment not exceeding six months or a fine of the third category.
2 Indien dit geschiedt door middel van geschriften of afbeeldingen, verspreid, openlijk tentoongesteld of aangeslagen, of door geschriften waarvan de inhoud openlijk ten gehore wordt gebracht, wordt de dader, als schuldig aan smaadschrift, gestraft met gevangenisstraf van ten hoogste een jaar of geldboete van de derde categorie.	**2** If such is done by means of written material, or images, which are either distributed, publicly displayed or posted, or by means of written material the contents of which are publicly uttered, the offender shall be guilty of libel and shall be liable to a term of imprisonment not exceeding one year or a fine of the third category.
3 Noch smaad, noch smaadschrift bestaat voor zover de dader heeft gehandeld tot noodzakelijke verdediging, of te goeder	**3** Neither slander nor libel shall exist if the offender's act was necessary in defence of his own or another person's interests or if he

trouw heeft kunnen aannemen dat het te last gelegde waar was en dat het algemeen belang de telastlegging eiste.	could have believed in good faith that the allegation was true and was required in the public interest.

Annex V – Article 262 Dutch Criminal Code (*Wetboek van Strafrecht*)

Artikel 262 Wetboek van Strafrecht	**Article 262 Dutch Criminal Code**
1 Hij die het misdrijf van smaad of smaadschrift pleegt, wetende dat het te last gelegde feit in strijd met de waarheid is, wordt, als schuldig aan laster, gestraft met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie. **2** Ontzetting van de in artikel 28, eerste lid, onder 1° en 2°, vermelde rechten kan worden uitgesproken.	**1** Any person who commits the serious offence of slander or of libel, knowing that the allegation is untrue, shall be guilty of aggravated defamation and shall be liable to a term of imprisonment not exceeding two years or a fine of the fourth category. **2** Disqualification from the rights listed in section 28(1)(1°) and (2°) may be imposed.

Annex VI – Article 284 Dutch Criminal Code (*Wetboek van Strafrecht*)

Artikel 284 Wetboek van Strafrecht	**Article 284 Dutch Criminal Code**
1 Met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie wordt gestraft: **1°** hij die een ander door geweld of enige andere feitelijkheid of door bedreiging met geweld of enige andere feitelijkheid, gericht hetzij tegen die ander hetzij tegen derden, wederrechtelijk dwingt iets te doen, niet te doen of te dulden; **2°** hij die een ander door bedreiging met smaad of smaadschrift dwingt iets te doen, niet te doen of te dulden. **2** In het geval onder 2° omschreven wordt het misdrijf niet vervolgd dan op klacht van hem tegen wie het gepleegd is.	**1** Any person who: **1°** unlawfully compels another person to act or to refrain from certain acts or to tolerate certain acts by an act of violence or any other act or by threat of violence or threat of any other act, either directed against that other or against others; **2°** compels another person to act or to refrain from certain acts or to tolerate certain acts by the threat of slander or libel; shall be liable to a term of imprisonment not exceeding nine months or a fine of the third category. **2** In the case defined in 2°, prosecution of the serious offence shall take place only on complaint of the person against whom it was committed.

Annex VII – Article 285 Dutch Criminal Code (*Wetboek van Strafrecht*)

Artikel 285 Wetboek van Strafrecht	**Article 285 Dutch Criminal Code**
1 Bedreiging met openlijk in vereniging geweld plegen tegen personen of goederen, met geweld tegen een internationaal beschermd persoon of diens beschermde goederen, met enig misdrijf waardoor gevaar voor de algemene veiligheid van	**1** The threat of public violence jointly committed against persons or property, the threat of violence against an internationally protected person or his protected property or the threat of any serious offence endangering the general safety of persons or

personen of goederen of gemeen gevaar voor de verlening van diensten ontstaat, met verkrachting, met feitelijke aanranding van de eerbaarheid, met enig misdrijf tegen het leven gericht, met gijzeling, met zware mishandeling of met brandstichting, wordt gestraft met gevangenisstraf van ten hoogste twee jaren of geldboete van de vierde categorie.	property or resulting in general danger for the provision of services, of rape, of indecent assault, of any serious offence against the life of a person, of hostage-taking, of aggravated assault or of arson, shall be liable to a term of imprisonment not exceeding two years or a fine of the fourth category.
2 Indien deze bedreiging schriftelijk en onder een bepaalde voorwaarde geschiedt, wordt ze gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vierde categorie.	**2** If such threat is made in writing stating a specific condition, a term of imprisonment not exceeding four years or a fine of the fourth category shall be imposed.
3 Bedreiging met een terroristisch misdrijf wordt gestraft met gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie.	**3** Threat of a terrorist offence shall be punishable by a term of imprisonment not exceeding six years or a fine of the fifth category.
4 Indien het feit, omschreven in het eerste, tweede of derde lid, wordt gepleegd met het oogmerk om een terroristisch misdrijf voor te bereiden of gemakkelijk te maken, wordt de op het feit gestelde gevangenisstraf met een derde verhoogd.	**4** If the offence defined in subsections (2) or (3) is committed with the intention of preparing or facilitating a terrorist offence, the term of imprisonment prescribed for the offence shall be increased by one third.

Annex VIII – Article 285b Dutch Criminal Code (*Wetboek van Strafrecht*)

Artikel 285b Wetboek van Strafrecht	**Article 285b Dutch Criminal Code**
1 Hij, die wederrechtelijk stelselmatig opzettelijk inbreuk maakt op eens anders persoonlijke levenssfeer met het oogmerk die ander te dwingen iets te doen, niet te doen of te dulden dan wel vrees aan te jagen wordt, als schuldig aan belaging, gestraft met een gevangenisstraf van ten hoogste drie jaren of een geldboete van de vierde categorie.	**1** Any person who unlawfully, systematically, intentionally violates another person's personal privacy with the intention of compelling that other person to act or to refrain from certain acts or to tolerate certain acts or of instilling fear in that person, shall be guilty of stalking and shall be liable to a term of imprisonment not exceeding three years or a fine of the fourth category.
2 Vervolging vindt niet plaats dan op klacht van hem tegen wie het misdrijf is begaan.	**2** Prosecution shall take place only on complaint of the person against whom the serious offence has been committed.

Annex IX – Article 125p Dutch Code of Criminal Procedure (*Wetboek van Strafvordering*)

Artikel 125p Wetboek van Strafvordering	**Article 125p Dutch Code of Criminal Procedure**
1 In geval van verdenking van een misdrijf als omschreven in artikel 67, eerste lid, kan de officier van justitie aan een aanbieder van	**1** In case of suspicion of a crime as described in article 67, sub 1, the public prosecutor can order a communication

een communicatiedienst als bedoeld in artikel 138g het bevel richten om terstond alle maatregelen te nemen die redelijkerwijs van hem kunnen worden gevergd om bepaalde gegevens die worden opgeslagen of doorgegeven, ontoegankelijk te maken, voor zover dit noodzakelijk is ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten.	service provider as meant in article 138g to immediately take all the measures that reasonably can be required of him to make certain information that is stored or shared inaccessible, as far as this is necessary to stop a criminal offence from taking place or in order to prevent new criminal offences from taking place.
2 Het bevel, bedoeld in het eerste lid, is schriftelijk en vermeldt: **a** het strafbare feit; **b** de feiten en omstandigheden waaruit blijkt dat ontoegankelijkmaking van de gegevens noodzakelijk is om het strafbare feit te beëindigen of nieuwe strafbare feiten te voorkomen; **c** welke gegevens ontoegankelijk moeten worden gemaakt.	**2** The order, which is mentioned in sub 1, is written and mentions: **a** the criminal offence; **b** the facts and circumstances that prove that making the information inaccessible is necessary to stop the criminal offence or to prevent new criminal offences; **c** which information needs to be made inaccessible.
3 Artikel 125o, tweede en derde lid, zijn van overeenkomstige toepassing.	**3** Article 125, sub 2 and 3, shall apply mutatis mutandis.
4 Het bevel, bedoeld in het eerste lid, kan slechts worden gegeven na voorafgaande schriftelijke machtiging, op vordering van de officier van justitie te verlenen door de rechter-commissaris. De rechter-commissaris stelt de aanbieder tot wie het bevel is gericht in de gelegenheid te worden gehoord. De aanbieder is bevoegd zich bij het horen door een raadsman te doen bijstaan.	**4** The order, which is mentioned in sub 1, can only be given after a prior written authorisation, to be provided by the examining judge on request of the public prosecutor. The examining judge offers the provider to whom the order is directed to the possibility to be heard. The provider is able to be assisted by a lawyer when he is heard.

Annex X – Article 19 Dutch Copyright Law (*Auteurswet*)

Artikel 19 Auteurswet	**Article 19 Dutch Copyright Law**
1 Als inbreuk op het auteursrecht op een portret wordt niet beschouwd de verveelvoudiging daarvan door, of ten behoeve van, den geportretteerde of, na diens overlijden, zijne nabestaanden.	**1** Not regarded as an infringement of the copyright in a portrait is the reproduction of it by or on behalf of the person portrayed or after his death, of his relatives.
2 Bevat eene zelfde afbeelding het portret van twee of meer personen, dan staat die verveelvoudiging aan ieder hunner ten aanzien van andere portretten dan zijn eigen slechts vrij met toestemming van die andere personen of, gedurende tien jaren na hun overlijden, van hunne nabestaanden.	**2** If the same portrait represents two or more persons, for each of them the entitlement to reproduce the other persons portraits requires their permission, or, in the ten years after their death, the permission of their relatives.

3 Ten aanzien van een fotografisch portret wordt mede niet als inbreuk op het auteursrecht beschouwd het openbaar maken daarvan in een nieuwsblad of tijdschrift door of met toestemming van een der personen, in het eerste lid genoemd, mits daarbij de naam des makers, voor zoover deze op of bij het portret is aangeduid, vermeld wordt. **4** Dit artikel is slechts van toepassing ten aanzien van portretten, welke vervaardigd zijn ingevolge eene opdracht, door of vanwege de geportretteerde personen, of te hunnen behoeve aan den maker gegeven.	**3** Where it concerns a photographic portrait, it is not regarded as an infringement of the copyright if the portrait is made public in a newspaper or periodical by or with the consent of one of the persons referred to in the first paragraph provided the name of the maker is stated if the name is indicated on or with the portrait. **4** This Article only applies to portraits made on commission by or on behalf of the persons portrayed, or made on commission for their benefit.

Annex XI – Article 20 Dutch Copyright Law (*Auteurswet*)

Artikel 20 Auteurswet	**Article 20 Dutch Copyright Law**
1 Tenzij anders is overeengekomen is degene, wien het auteursrecht op een portret toekomst, niet bevoegd dit openbaar te maken zonder toestemming van den geportretteerde of, gedurende tien jaren na diens overlijden, van diens nabestaanden. **2** Bevat eene zelfde afbeelding het portret van twee of meer personen, dan is ten aanzien van de gansche afbeelding de toestemming vereischt van alle geportretteerden of, gedurende tien jaren na hun overlijden, van hunne nabestaanden. **3** Het laatste lid van het voorgaande artikel is van toepassing.	**1** Unless otherwise agreed, the owner of the copyright in a portrait is entitled to make it public without the consent of the person portrayed or, during the ten years after his death, without the consent of his relatives. **2** If an image contains the portrait of two or more persons, the consent of all the persons portrayed is required, or, during the ten years following their death, the consent of their relatives. **3** The last paragraph of the preceding Article applies.

Annex XII – Article 21 Dutch Copyright Law (*Auteurswet*)

Artikel 21 Auteurswet	**Article 21 Auteurswet**
Is een portret vervaardigd zonder daartoe strekkende opdracht, den maker door of vanwege den geportretteerde, of te diens behoeve, gegeven, dan is openbaarmaking daarvan door dengene, wien het auteursrecht daarop toekomst, niet geoorloofd, voor zover een redelijk belang van den geportretteerde of, na zijn overlijden, van een zijner nabestaanden zich tegen de openbaarmaking verzet.	If a portrait is made without the maker having been commissioned by or on behalf of the persons portrayed, or having been commissioned for their benefit, the copyright owner is not permitted to make the portrait public if there is a reasonable interest against publication on the part of the person portrayed or, after his death, of one of his relatives.

Annex XIII – Article 35 Dutch Copyright Law (*Auteurswet*)

Artikel 35 Auteurswet	**Article 35 Dutch Copyright Law**
1 Hij die zonder daartoe gerechtigd te zijn een portret in het openbaar ten toon stelt of op andere wijze openbaar maakt, wordt gestraft met geldboete van de vierde categorie. **2** Het feit is eene overtreding.	**1** He who exhibits a portrait in public or makes it public in any other manner, without being authorised to do so, is punishable by a fine of the fourth category. **2** The act is an offence.

Annex XIV – Article 17 General Data Protection Regulation (*Algemene Verordening Gegevensbescherming*)

Article 17 General Data Protection Regulation
1 The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies: **a** the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; **b** the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing; **c** the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2); **d** the personal data have been unlawfully processed; **e** the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject; **f** the personal data have been collected in relation to the offer of information society services referred to in Article 8(1). **2** Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data. **3** Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: **a** for exercising the right of freedom of expression and information; **b** for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; **c** for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3); **d** for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or **e** for the establishment, exercise or defence of legal claims.

Annex XV – Article 6 General Data Protection Regulation (*Algemene Verorderning Gegevensbescherming*)

Article 6 General Data Protection Regulation
1 Processing shall be lawful only if and to the extent that at least one of the following applies: **a** the data subject has given consent to the processing of his or her personal data for one or more specific purposes; **b** processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; **c** processing is necessary for compliance with a legal obligation to which the controller is subject; **d** processing is necessary in order to protect the vital interests of the data subject or of another natural person; **e** processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; **f** processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child. Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks. **2** Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX. **3** The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by: **a** Union law; or **b** Member State law to which the controller is subject. The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. 3That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. 4The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued. **4** Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law

which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:
a any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
b the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
c the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
d the possible consequences of the intended further processing for data subjects;
e the existence of appropriate safeguards, which may include encryption or pseudonymisation.

Bibliography

Articles

B. Chesney & D. Citron, 'Deep Fakes: A Looming Challenge for Privacy, Democracy and National Security' (2019) 107 California Law Review 1753.

D. Citron, 'Sexual Privacy' (2018) 25 University of Maryland Francis King Carey School of Law Legal Studies Research Paper 1870. Available on SSRN: http://ssrn.com/abstract=3233805 (last accessed on 18 April 2020).

R.A. Delfino, 'Pornographic Deepfakes – Revenge Porn's Next Tragic Act – The Case for Federal Criminalization' (2019) 88 Fordham Law Review 887.

European Data Protection Board, 'Guidelines 5/2019 on the criteria of the Right to be Forgotten in the search engine cases under the GDPR (part 1)' (2019). Access online: https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2019/guidelines-52019-criteria-right-be-forgotten-search_en (last accessed on 18 April 2020).

F. Eshragh *et al.*, 'Automated negotiation in environmental resource management: Review and assessment' (2015) 162 Journal of Environmental Management 148.

K. Farish, 'Do deepfakes pose a golden opportunity? Considering whether English law should adopt California's publicity right in the age of deepfake' (2020) 15 Journal of Intellectual Property Law & Practice 40.

FRA/ECtHR/EDPS, Handbook on European Data Protection Law (2018). Access online: https://fra.europa.eu/en/publication/2018/handbook-european-data-protection-law-2018-edition (last accessed on 18 April 2020).

M.A. Franks, 'Criminalizing Revenge Porn: Frequently Asked Questions' (2013). Available on SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2337998 (last accessed on 18 April 2020).

I.J. Goodfellow *et al.*, 'General Adversarial Nets' (2014) 2 NIPS'14: Proceedings of the 27th International Conference on Neural Information Processing Systems 2672.

M. Goudsmit, 'Criminalising Image-based Sexual Abuse: an Analysis of the Dutch Bill against Revenge Pornography' (2019) 68 Ars Aequi 442.

M. Goudsmit, 'De wijzende vinger bekeken: Over de strafbaarstelling van wraakpornografie' (2018) 24 NJB 1721.

D. Harris, 'Deepfakes: False Pornography is Here and the Law cannot Protect You' (2019) 17 Duke Law & Technology Review 99.

S. van der Hof, 'Wraakporno op Internet' (2016) 65 Ars Aequi 54.

H.K. Hull, 'When Seeing Isn't Believing' (2019) 27 Catholic University Journal of Law and Technology 51.

M-H. Maras & A. Alexandrou, 'Determining the authenticity of video in the age of artificial intelligence and in the wake of Deepfake videos' (2019) 23 The International Journal of Evidence & Proof 255.

C. Öhman, 'Introducting the pervert's dilemma: a contribution to the critique of Deepfake Pornography' (2019) Ethics and Information Technology. Access online: https://rdcu.be/b3DZM (last accessed on 18 April 2020).

D. Stewart & K. Bunton, 'Practical Transparency: How Journalists Should Handle Digital Shaming and "The Streisand Effect"' (2016) 5 Journal of Media Law & Ethics 4.

S.R. Stroud & J. Henson, 'What Exactly is Revenge Porn or Nonconsensual Pornography?' (2016). Available on SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2828740 (last accessed on 18 April 2020).

J.M. ten Voorde, 'Vervaardigen enz. van afbeelding van seksuele aard' (2020) T&C Strafrecht, commentaar op art. 139h Sr. Access online: https://www.navigator.nl/document/idpassec16055901db4dc4a1b1827e3061c72e?ctx=WKNL_CSL_581 (last accessed on 23 May 2020).

S. Vosoughi *et al.*, 'The spread of true and false news online' (2018) 359 Science 1146.

T. Wagner & A. Blewer, '"The World Is No Longer Real": Deepfakes, Gender, and the Challenges of AI-Altered Video' (2019) 3 Open Information Science 32.

M. Westerlund, 'The Emergence of Deepfake Technology: A Review' (2019) 9 Technology Innovation Management Review 39.

Case law

European Court of Justice

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

European Court of Human Rights

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

High Court of the Netherlands

HR 1 July 1988, NJ 1988/1000.

HR 12 March 2013, ECLI:NL:HR:2013:BY9719.

HR 24 June 2014, ECLI:NL:HR:2014:1497.

Court of Appeal of the Netherlands

Hof Leeuwarden 4 May 2010, ECLI:NL:GHLEE:2010:BM3169.

Hof Amsterdam 19 October 2017, ECLI:NL:GHAMS:2017:4648.

Hof Den Haag 13 June 2018, ECLI:NL:GHDHA:2018:2017.

District Court of the Netherlands

Rb. Leeuwarden 9 April 2009, ECLI:NL:GHLEE:2010:BM3169

Rb. Gelderland 30 March 2018, ECLI:NL:RBGEL:2018:1461.

Explanatory reports

The Netherlands

Kamerstukken I, 2001/02, 27745, 299b.

Kamerstukken I, 2001/02, 27745 (memorie van antwoord).

Kamerstukken II, 2000/01, 27745, 3.

Kamerstukken II, 2001/02, 27745, 6.

Kamerstukken II, 2018/19, 35080, 3.

Governmental Documents

The Netherlands

K.H. Ollongren, 'Brief inzake desinformatie en beïnvloeding verkiezingen' (2018). Access online: https://www.rijksoverheid.nl/documenten/kamerstukken/2018/12/13/kamerbrief-over-dreiging-desinformatie-en-beinvloeding-verkiezingen (last accessed on 25 April 2020).

Legislation

Council of Europe

Cybercrime Convention.

European Union

General Data Protection Regulation.

The Netherlands

Dutch Code of Criminal Procedure (*Wetboek van Strafvordering*).

Dutch Copyright Law (*Auteurswet*).

Dutch Criminal Code (*Wetboek van Strafrecht*).

United States

Code of Virginia, §18.2-362.2 'Unlawful dissemination or sale of images of another; penalty'. Access online: https://law.lis.virginia.gov/vacode/18.2-386.2/ (last accessed on 18 April 2020).

News articles

M. Fertik, 'Your Future Employer Is Watching You Online. You Should Be, Too' (3 April 2012) Harvard Business Review. Access online: https://hbr.org/2012/04/your-future-employer-is-watchi (last accessed on 26 April 2020).

J. Haspels, 'Anne, slachtoffer van wraakporno, ging door hel: "Rechtzaak ter afsluiting"' (28 April 2018) AD. Access online: https://www.ad.nl/den-haag/anne-slachtoffer-van-wraakporno-ging-door-hel-rechtszaak-ter-afsluiting~afb59ccd/?referrer=https://www.google.nl/ (last accessed on 26 April 2020).

J. Koebler & J. Cox, 'The Impossible Job: Inside Facebook's Struggle to Moderate Two Billion People' (23 August 2018) VICE Motherboard. Access online: https://www.vice.com/en_us/article/xwk9zd/how-facebook-content-moderation-works (last accessed on 26 April 2020).

L. Matsakis, ‘Artificial Intelligence Is Now Fighting Fake Porn’ (14 February 2018) WIRED. Access online: https://www.wired.com/story/gfycat-artificial-intelligence-deepfakes/ (last accessed on 2 April 2020).

C. Newton, ‘The Trauma Floor: The secret lives of Facebook moderators in America’ (25 February 2019) The Verge. Access online: https://www.theverge.com/2019/2/25/18229714/cognizant-facebook-content-moderator-interviews-trauma-working-conditions-arizona (last accessed on 23 May 2020).

J. Schellevis, ‘Zorgen OM over deepfakes: “Risico op oplichting en afpersing”’ (7 September 2019) NOS. Access online: https://nos.nl/artikel/2300688-zorgen-om-over-deepfakes-risico-op-oplichting-en-afpersing.html (last accessed on 18 April 2020).

Shownieuws, ‘Bridget Maasland slachtoffer van deepfake-porno’ (4 March 2020) Shownieuws. Access online: https://www.shownieuws.nl/video/clips/2020/bridget-slachtoffer/ (last accessed on 13 May 2020).

T. Tates, ‘Manager woest na opduiken deepfake-pornofilmpje Dionne Stax: “Aangifte in voorbereiding”’ (27 August 2019) AD. Access online: https://www.ad.nl/binnenland/manager-woest-na-opduiken-deepfake-pornofilmpje-dionne-stax-aangifte-in-voorbereiding~af9dace5/ (last accessed on 28 April 2020).

E. Thomas, ‘In the battle against deepfakes, AI is being pitted against AI’ (25 November 2019) WIRED. Access online: https://www.wired.co.uk/article/deepfakes-ai (last accessed on 25 April 2020).

V. Turk, ‘Deepfakes are already breaking democracy. Just ask any woman.’ (18 November 2019) WIRED. Access online: https://www.wired.co.uk/article/deepfakes-pornography (last accessed on 16 April 2020).

De Volkskrant, ‘Slachtoffer wraakporno heeft recht op gegevens Facebook’ (25 June 2020). Access online: https://www.volkskrant.nl/cultuur-media/slachtoffer-wraakporno-heeft-recht-op-gegevens-facebook~bcf82389/ (last accessed on 26 April 2020).

De Volkskrant, ‘Slachtoffer en Facebook schikken in wraakpornozaak’ (3 March 2016). Access online: https://www.volkskrant.nl/nieuws-achtergrond/slachtoffer-en-facebook-schikken-in-wraakpornozaak~bda81aef/?referer=https%3A%2F%2Fwww.google.nl%2F (last accessed on 26 April 2020).

Reports

Deeptrace, ‘The State of Deepfakes’ (2019). Access online: https://storage.googleapis.com/deeptrace-public/Deeptrace-the-State-of-Deepfakes-2019.pdf (last accessed on 18 April 2020).

Other sources

Council of Europe, ‘Chart of signatures and ratifications of Treaty 185 – Convention on Cybercrime’. Access online: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=RnKq5xsu (last accessed on 17 April 2020).

Deepfake Detection Challenge. Access online: https://deepfakedetectionchallenge.ai/ (last accessed on 6 April 2020).

Deepfakes Web, https://deepfakesweb.com/ (last accessed on 13 May 2020).

Facebook, ‘Enforcing Against Manipulated Media’ (6 January 2020). Access online: https://about.fb.com/news/2020/01/enforcing-against-manipulated-media/ (last accessed on 6 April 2020).

A. Hauser, ‘Deepfake Analysis: Amount of Images, Lighting and Angles’ (22 November 2018) SCIP. Access online: https://www.scip.ch/en/?labs.20181122 (last accessed on 13 May 2020).

Helpwanted.nl, https://www.helpwanted.nl/ (last accessed on 14 May 2020).

MachineTube, https://www.machine.tube/ (last accessed on 13 May 2020).

Reddit, ‘Do not impersonate an individual or entity’ (date unknown). Access online: https://www.reddithelp.com/en/categories/rules-reporting/account-and-community-restrictions/do-not-impersonate-individual-or (last accessed on 26 April 2020).

Tor Project, https://www.torproject.org/about/history/ (last accessed on 16 April 2020).

Twitter, ‘Building rules in public: Our approach to synthetic & manipulated media’ (4 February 2020). Access online: https://blog.twitter.com/en_us/topics/company/2020/new-approach-to-synthetic-and-manipulated-media.html (last accessed on 7 April 2020).