VIRTUAL REVENGE PORNOGRAPHY AS A NEW ONLINE THREAT TO SEXUAL INTEGRITY

Miha ŠEPEC

E-mail: miha.sepec@um.si
Associate professor, Faculty of Law Maribor,
University of Maribor

Melanija LANGO

E-mail: melanija.lango@gmail.com
Expert associate at Investment Banking and Custody Department, Nova KBM d.d., Maribor
And
Judicial trainee, Higher Court in Maribor

Abstract

Non-consensual pornography, better known under its popular name of revenge pornography, is one of the new forms of cybercrime offences. Revenge pornography refers to non-consensual dissemination of intimate images taken with the consent of an individual but with the implicit expectation that these images would remain private. Several countries around the world have taken measures to combat this cyber phenomenon and at this point, most of them more or less effective in an effort to criminalize it. However, as with all cybercrimes, the technology is continuously evolving and the perpetrators are always one step ahead of the legislators thinking of new better ways of breaking the law and blurring the line between legal and illegal.

With new artificial intelligence(hereafter: AI) algorithm technology that enables anyone to create a so-called "deepfake" video, in which a person in an existing image or video is replaced with someone else's likeness using artificial neural networks, new doors for misuse and online disinformation are opening. The technology can be used to manipulate and sow misinformation among voters in political campaigns and media, but also to make fake (virtual) pornographic videos. The article analyses and compares current revenge pornography legislation in selected countries, trying to answer the question if it can be applied and effectively used to protect personal and sexual integrity of an individual who is victimized by this new phenomenon. Virtual revenge pornography poses some new legal questions. What type of

rights are being violated? Is it a person's privacy, reputation, or sexual integrity? The article aims to contemplate these and other relevant questions that may pose a hurdle to efficiently criminalizing virtual revenge pornography in the future.

Key words: *deepfake, artificial intelligence (AI), internet, social networks, cybercrime, revenge pornography*

1. Introduction

In the new millennium, also called the digital information age, computer-information systems have completely changed our society. The technological-information revolution has dramatically affected human relations, especially in the field of communications. Digital communication and the internet have completely changed the functioning of our society. The development of new technologies, unfortunately, has spawned various forms of behaviour that are contrary to legally desirable behaviour. In the field of digital technologies, new criminal offences are emerging, classified as cybercrimes (Jaishankar, 2018, p.1). One such new crime is the publication and dissemination of images with sexual content of others without their consent on the World Wide Web or through public digital channels and applications, often referred to as "revenge pornography" or "non-consensual pornography." As with child pornography, this crime can be classified as a content-related cybercrime (Clough, 2015, p. 287; Šepec, 2018, p. 6).

The term revenge pornography refers to non-consensual dissemination of intimate images taken with the consent of an individual but with the implicit expectation that these images will remain private, though the term "revenge pornography," can be somewhat misleading. In many cases, the primary motivation of the perpetrators is not revenge, so some suggest using the term non-consensual pornography instead (Citron & Franks, 2014, p. 349). The latter has a broader significance and is defined as the distribution of sexually graphic images of individuals without their consent. "This includes images originally obtained without consent, e.g. by using hidden cameras, hacking phones, or recording sexual assaults, as well as images obtained with the consent in an intimate relationship with the victim" (Franks, 2013, p. 1). For the purpose of this article, the better-known term revenge pornography will be used, although the question of consent will be prevalent through the article.

Revenge pornography is classified as a content-related crime on information systems. These crimes include digital content that is published online or misused with a computer system and is criminalized because of the content itself. Some offences are related to copyright violations, while others include child pornography and other forms of illegal pornography (Wall, 2015, p.80). Although the content of a revenge pornography video as such may not be questionable, since adult pornography is legal in most countries, from the

legal point of view, the content is problematic because it is distributed without the consent of the victim and thus represents an intrusion into privacy of the individual in the image, therefore attacking his personal and sexual integrity.

Israel was the first country to criminalize revenge pornography (Burris, 2014, p. 2332). Most of the countries around the world followed suit and criminalized it more or less successfully.

Four different approaches to criminalization of revenge pornography as a complex and multifaceted crime can be identified in the countries with revenge pornography legislation:

1) The criminalization of non-consensual disclosure of private, sexual images or films that have been specifically made with consent;
2) The criminalization of non-consensual disclosure of private, sexual images or films made either with or without consent;
3) The criminalization of non-consensual disclosure of private, sexual images or films made without consent, with the presupposition that this criminalizes revenge pornography;
4) No effective laws are in place, despite what countries might believe to be the case (Goudsmit, 2017, p. 14).

There are some similarities and some distinct differences between these approaches and it is hard to characterize one approach as more suitable than the other, as the biggest problem with revenge pornography is its multifacetedness and complexity, making it hard to find an all-around effective approach to criminalization. At first glance, it may seem that criminalizing these online submissions is relatively straightforward, but as a cybercrime, it is ever evolving, and the perpetrators always seem to be one step ahead of the legislator. The legislator's task is, above all, to pay attention to advances in the field of information technology and to remain sufficiently critical and especially mindful of the open questions not yet regulated by legislation.

Revenge pornography is a form of cybercrime and as such, it is always presenting new challenges for the legislator, the latest, it seems, might lie in the rise of AI, deep learning, and image processing which enables the creation of so-called "deepfake" videos. The technology enables the perpetrator to successfully alter images, video, or audio (or even create them from scratch) in a way that is highly realistic and difficult to detect (Chesney & Citron, 2019, p. 1757). With deep learning technology that is used for deepfakes, pairs of algorithms are pitted against each other in "generative adversarial networks," or GANS. In a GAN, one algorithm, the "generator," creates content modelled on source data, e.g. creating artificial images of dogs from a database of real dog photos, while a second algorithm, the "discriminator",

tries to detect the artificial content, to pick out the fake dog photos. GANS can produce extremely realistic yet false audio and video content. As it is constantly training one against the other, such pairings can lead to rapid improvement (Chesney & Citron,2019, p. 1760). This technology can also be used to impose one person's face onto another person's body, enabling the creation of so-called pornographic deepfakes. In fact, the term "deepfake" came from a Reddit user who first employed the technology to create pornographic videos (Hall, 2018, p. 58*)*.

As of 2015, when Google released Tensor Flow, its "internal tool for developing artificial intelligence algorithms" (Gershgron, 2018), the technology is available to the public. With the help of the tutorials accessible online one can create deepfakes from the comfort of one's own home with relative ease, requiring only a computer with a proper graphics card, the FakeApp program, which uses the open-source software released by Google, and hundreds of photos of a person, known as a "faceset". Creating such videos is increasingly easy as even finding a body that matches the victim's face has become quasi-automated. Browser-based applications employing facial recognition software enable users to upload a photo of the person they want in the fake video, and the website outputs the most similar adult performer (Harris, 2018, p.101). From its early days, the technology was used for deviant purposes, primarily for adding celebrity faces to porn stars, but as quickly as it became more accessible to the public, the people featured in these videos become non consenting normal individuals.

This article will focus on deepfake pornographic videos used as revenge pornography and will examine the legal issues and questions stemming from such misuse, using a comparative analysis of revenge pornography legislation around the world. In this article, these pornographic deepfake videos will be referred to as "virtual revenge pornography", the reason for the proposed use of this term will also be discussed.

2. The Modern-Day Dilemmas of Revenge Pornography

With the advances of technology, the computer-generated images are becoming more and more realistic. Consequently, it is becoming exceedingly difficult for inexperienced observers to make the distinction between the virtual and the real. When comparing an "old fashion" revenge pornography image and the new virtual revenge pornography image, some remarkable similarities can be seen. Both forms are non-consensual as the images of the victims are distributed without their consent, both can cause intense distress, humiliation, shame, anger, guilt, paranoia, depression, which could even result in suicide (Kamal & Newman, 2016, p. 362). The mental health implications of revenge pornography and virtual revenge pornography are similar for the victim, due to the fact that it is highly unlikely that the general

observer will believe the victim's claims that the image was digitally generated. The victim in both cases is sexually objectified and humiliated in front of thousands of people online and once these images are published on the World Wide Web it is almost impossible to erase them. At the same time, one cannot negate the obvious differences in cases where the images are unquestionably fraudulent. Virtual revenge pornography, as such, has in the past been viewed and used as a form of entertainment and artistic expression rather than a crime. It is believed that virtual revenge pornography cannot raise the same level of sexual privacy concerns, as it does not depict a person who actually exists', consequently it is impossible for an individual's privacy to be violated. However, this argument does not hold in the case of unidentified individual whose face was used to create a realistic sexual image of him or her, as the viewers may not apprehend the video depiction as fraudulent and may instead believe that the video is a genuine depiction of a real person. The pool of potential victims of virtual revenge pornography is therefore limitless as the face of anyone whose image has been captured digitally can be used to create it. In a way, this means that, as opposed to revenge pornography where an individual can protect himself/herself by not appearing in sexually explicit digital images, the victims of virtual revenge pornography do not have the same luxury (Delfino, 2019, p. 897-898). Another dilemma of virtual revenge pornography is who the victim there really is as two different people appear in these videos. It is correct to conclude that the person whose face was used did not agree to participate in pornography, but at the same time, the consent was also not given by the pornographic actor whose body was used to have another person's face superimposed onto his or her body. Should both people depicted in the virtual revenge pornography be presumed to be victims (Delfino, 2019, p. 898)? Or will the victim only be the one whose face was used? As a body in itself normally cannot be used to identify a certain person, who could be victimized with the use of virtual pornography. An exception to this rule would be athletes, models, and actors that have a specific body or body characteristics, that can generally be used to identify the person of the body.

To fully understand the nature of virtual revenge pornography one has to first answer the question: what does revenge pornography legislation aim to punish and which legal interest does it protect? A breach of privacy or sexual humiliation of victims? Is revenge pornography a privacy violation offence or a sexual crime? When looking at virtual revenge pornography as a sexual crime one might argue there is an uncanny similarity with virtual child pornography, where the possession, distribution of these types of virtual images is criminalized in most countries. In answer to these questions, the use of the term "virtual revenge pornography" seems more fitting in describing this virtual phenomenon than deepfake pornography. Virtual revenge pornography has some similarities to virtual child pornography, where it is necessary to shut down the "distribution network" of child pornography and

therefore to reduce the sexual exploitation of children (Citron &Franks, 2014, p. 364).However, one might ask whether there really is a legal argument to exclude the protection of digitally altered images of adults (Pegg, 2018, p. 13)?

Most European countries have characterized revenge pornography as a privacy offence. In England and Wales, it is even an offence of private disclosure. The characterization of revenge pornography as a sexual offence is relatively rare in Europe, but in the majority of American states, revenge pornography is seen as a sexual offence.

The main reason that virtual child pornography is criminalized in most European countries is the belief that by its nature it might incite criminal activity and can be used as an aid to paedophiles in grooming children. As such images also depict children in a sexually explicit way, it is believed that it can have the potential for exploitation of children. There are various theoretical justifications for criminalizing virtual child pornography, one of them being protection of public morality (Byberg,2012, p.29). In Ashcroft v. The Free Speech Coalition, the U.S. Supreme Court held that the government must not criminalize such action because the production of "virtual child" pornography does not sexually abuse an actual child (Ashcroft v. The Free Speech Coalition, 122 S. Ct. 1389, 2002).With that decision, The Court rejected the government's argument and the position that most European countries criminalize "virtual child" pornography because it encourages paedophiles to abuse children. The court's decision must undoubtedly be taken in the cultural context as the US First Amendment, which affords abroad protection of free speech. Virtual child pornography in US is defined in the PROTECT Act which classifies it only as obscene content. In other words, one can be brought to court on an obscenity charge, not a child pornography charge, for creating or possessing computer-generated child pornography, where no actual children were involved in creating the pornography (Byberg, 2012, p.21). While one can argue that most of the arguments for the criminalization of virtual child pornography cannot be successfully transferred to the criminalization of virtual revenge pornography of adults, as the law primarily aims to protect the children from potential perpetrators, the argument of protecting public morality can also be applicable to virtual revenge pornography. Although current laws on revenge pornography, as will be seen in the next section, might be used for the prosecution of virtual revenge pornography, these laws have their own limitations as technology is becoming more refined and virtual revenge pornography videos are easier to create. Although the criminal legislation on virtual revenge pornography is currently still under discussion around the globe, some websites and social media giants have already taken their stand. PornHub has banned virtual revenge pornography videos, while similar bans were placed on Twitter and GIF-hosting site Gfycat. Reddit also closed down

the primary subreddit hosting virtual revenge porn, but it was deemed mostly futile as users migrate the material to other locations.

For successful regulation of virtual revenge pornography, the law must be up to speed with modern technology. Proper criminalization of these new cybercrimes is important, as the victims will need proper channels to protect themselves from this new cultural phenomenon.

3. Comparative Analysis of Virtual Revenge Pornography

This chapter is a short analysis of the current revenge pornography laws in selected countries, examining the shortcomings and limitations for the criminalization of virtual revenge pornography. Existing revenge pornography laws will be examined as to whether they suffice for effectively bringing the perpetrators to justice.

Revenge pornography is criminalized in paragraph VI of Article 143 of Slovenian Criminal Code (2017), which stipulates[1] that anyone who publicly announces recordings or messages of another person with sexual content without the consent of that person and thereby seriously affects his or her privacy shall be punished by imprisonment of three months up to three years.

As the formulation of the article is quite broad,virtual revenge pornography could fall under this provision, as one could argue that it is indeed a recording of another person with sexual content, published without the consent of the person. The problem lies in the legal demand to seriously affect that person's privacy. The legal condition, namely "seriously affects his or her privacy," is the consequence of the perpetrator's act, which the perpetrator must be aware of and will it (direct intent), or at least consent to it, *dolus eventualis*, and does not constitute an objective condition of criminality or strict liability. In doing so, whether the individual's privacy rights have been adversely violated is assessed in the same way as defamation. This means that the violation of privacy must be objective, but it is not necessary that the victim subjectively felt seriously affected. Victims who do not feel their privacy was seriously violated, will probably not press charges for the prosecution of the crime, which can also be said if the person is mentally less developed, emotionally thawed or an exhibitionist. Whether a recording or message can objectively cause severe impairment must be assessed according to the time, circumstances, habits, persons and other socially relevant circumstances (Deisinger, 2002, p. 181). Nevertheless, what is the legal meaning of the phrase "seriously affects his or her privacy"? If the legislator explicitly

[1]Where no offical translation is available, translations will be provided by the authors of the Article.

requires that images are of sexual content, the privacy of a person in them will practically always be objectively affected. The perpetrator who publishes such images is surely aware that the person's privacy will also be affected by the publication of the images. Perhaps, therefore, the entire legal condition is unnecessary. Furthermore, it can bequite hard to prove that the main goal of the perpetrator is to seriously affect the privacy of the individual, but one could argue that if others believe that the video is a genuine depiction of that person, the person's privacy could be seriously affected and that the perpetrator was aware of this. This is especially true when the content of the images is sexual.

In the Croatian Criminal Code (2011, official translation) revenge pornography can be found in chapter XIV titled "Crimes against Privacy".It is stipulated in the first paragraph of Article 144 (Unauthorized Taking of Pictures) that"Whoever, without authorisation, takes pictures of another person located in a dwelling or an area especially protected from view or uses or makes available to a third party such a picture and thereby violates that person's privacy shall be punished by imprisonment not exceeding one year." The problematic part of the given formulation, apart from the privacy issue already discussed, is the requirement that the unauthorized image of another must be created in an apartment or a space specifically protected from viewing. One could argue that revenge virtual revenge pornography videos are in most cases created in an apartment or space specifically protected from viewing, although this is not always the case. There are no persuasive arguments why a depiction of a sexual act in the woods or a park hidden from public view would not receive equal protection as a depiction of a sexual act in an apartment. Nevertheless,the offence as formulatednow can still be used to protect against virtual revenge pornography in most cases.

The first paragraph of Article 145 of the Serbian Criminal Code (2016, Translated by OSCE), titled "Unauthorised Publication and Presentation of Another's Texts, Portraits and Recordings", stipulates that

> Whoever publishes or publicly presents another's text, portrait, photograph, film or a phonogram of a personal character without the consent of a person who has drawn up the text or to whom it is related, or without consent of the person depicted on the portrait, photograph or film or whose voice is recorded on a phonogram, or without consent of the person whose consent is mandatory by law and thereby significantly violates the private life of that person, shall be punished with a fine or imprisonment up to one year.

The creation of such images or recordings is a criminal offense according to Article 144. Again,this is purely a privacy violation offence classified in Chapter XIV titled "Crimes against the Basic Human Rights". Apart from the

demand to significantly violate the private life of that person, which depends on the situation and must be proven in the court of law, the formulation is broad enough to include virtual revenge pornography.

Article 201a (Violation of intimate privacy by taking photographs) of the German Criminal Code (StGB, official translation, 2019) stipulates that:

> Whoever without being authorised to do so creates or transmits photographs or other images of another person in private premises or in a room which is specially protected from view, and thereby violates the intimate privacy of the person depicted, incurs a penalty of imprisonment for a term not exceeding two years or a fine.The same penalty is provided when the perpetrator without being authorised to do so produces a photograph or other image exhibiting the helplessness of another person or transmits such image, and thereby violates the intimate privacy of the person depicted. The sentence is the same ifperpetratoruses a photograph or other image produced by an offence under no. 1 or no. 2 or makes it available to a third party. It is also punishable to without being authorised to do so, make available to a third party a photograph or other image of another person, which is of such a nature as to significantly damage the reputation of the person depicted, it incurs the same penalty.

This is essentially child pornography. The article prohibits the perpetrator fromcreating a pictureof another person located in a dwelling or a room especially protected from view without authorization of that person. When it comes to virtual revenge pornography the verb "creates" can apply to the creation of the video, though in compliance with the article, such a picture must depict that person in a dwelling or a room especially protected from view, limiting virtual revenge pornography to selected videos depicting given spaces.

In Spain, revenge pornography is criminalized in the Penal Code of Spain (2015) Chapter X (Rights against Personal Dignity) where the seventh paragraph of Article 197 stipulates the following: If an individual, without the authorization of the person concerned, disseminates, discloses or transfers to third parties images or audio-visual recordings of the person concerned that have been obtained with the consent of the person at the place of residence or any other place away from the sight of others, he shall be punished with imprisonment of three months up to one year or a fine, or with six to twelve months imprisonment when the disclosure would seriously undermine the personal privacy of that person.

The formulation at hand is not the best for the criminalization of virtual revenge pornography as it specifically stipulates that the images or audio-

visual recordings must be obtained with the consent of the person. That is quite unlikely with virtual revenge pornography, where the images from which the fake digital content is created are commonly gained from public sources. Furthermore, the legislation explicitly prohibits obtaining of images or audio-visual recordings, and not virtually created content, as is the case with virtual revenge pornography.

In France, pursuant to Article 226-2 of the French Penal Code modified by Digital Republic Law (2016), non-consensual sharing with the public or a third party of any recording or document relating to words or images of a sexual nature obtained with the express or presumed consent of the person by recording, fixation, or transmission, shall be punished with up to 2 years of imprisonment and up to 60.000 euros fine. The French law is limitedregarding virtual revenge pornography, as the recordings must be obtained with the express or presumed consent of the person in the recording, fixation, or transmission. The first problem is similar to Spanish legislation,as the images must be obtained with consent or presumed consent, which is normally not applicable to virtual revenge pornography.The second limitation is that the recording must be obtained by recording, fixation or transmission; none of these are applicable for creation of virtual revenge pornography.

Until 2019, Italy has not enacted any specific laws or criminal law articles regulating revenge pornography. Limited protection was offered, however, both through the Data Protection Code (2003) and the libel and slander offences of the Penal Code (2015). In July 2019, Italy adopted a new act named "Codice rosso" in order to regulate various forms of sexual violence, especially against women. "Codice rosso" introduces Article 612 into the Italian Criminal Code regulating the distribution of pornographic images and videos, the so-called "revenge pornography". Article 612 stipulates, in the first paragraph, that anyone, after recording or stealing, sending, donating, selling, posting or distributing images or videos of a person with explicit sexual content, that is allegedly private, without the consent of that person, shall be punished with a prison sentence of one to six years and a fine of between 5,000 and 15,000 euros. The second paragraph of the same article also punishes with the same penalty those who have received or otherwise obtained the pictures or videos referred to in the first paragraph, and who send, donate, sell, publish or distribute them without the consent of the displayed persons, in order to cause them harm. The Italian formulation is broad enough and without any special restrictions and as such can be successfully used for virtual revenge pornography as well. The only requirement is that the content must be sexual so the person must be depicted in pornographic videos or videos of similar nature. Italian legislations, therefore, seems to be one of the most effective regarding virtual revenge pornography as it defines revenge pornography as a sexual offence and penalizes it with a very strict sentence.

In European countries, adhering to the continental criminal law doctrine, revenge pornography is primarily regarded as a privacy violationoffence,often not even demanding the content to be sexually explicit.The focus of continental criminal law systems is therefore on the violation of privacy – and not on the sexual integrity of the individual.The nature of virtual revenge pornography is such that itcan most definitely be stated that the victim's privacy is being violated even though the person, as opposed to the face, in the video might not be him or her.

The use of revenge pornography law for virtual revenge pornography might prove more problematic for Anglo-American law systems, where it is treated as sexual offence and is, as such,similar to child pornography, with the exception of England and Wales where it is only a private disclosure offence.

England and Wales Criminal Justice Act (2015) (hereafter, CJA) in section 33 stipulates that: "It is an offence for a person to disclose a private sexual photograph or film if the disclosure is made; without the consent of an individual who appears in the photograph or film, and with the intention of causing that individual distress." There is currently no specific law for virtual revenge pornography in England and Wales, as the CJA can be deemed unsuitable for virtual revenge pornography. The problem is within*mens rea* of the offence as it criminalizes only those who actively seek to humiliate or cause acute distress to the individual, and those whose ultimate goal is revenge. Section 33 (8) clarifies that solely because disclosure causes distress in the individual shownas a natural and probable consequence of the disclosure, this shall not be considered a crime if there is no actual intention of the offender to cause distress. Disclosure of images solely for sexual or financial gain, as well as disclosures to diminish an individual's reputation, would undoubtedly fall outside the well-defined *mens rea* of article 33 of the CJA. Consequently, most of the virtual revenge pornography wouldnot be successfully prosecuted.

In July 2019, Governor Andrew Cuomo signed a law criminalizing retaliatory pornography in New York. Thus, New York became the sixty-sixth state (in addition to Washington, D.C.) criminalizing revenge pornography. Only four USA states currently have no laws against revenge pornography (Ellis, 2019). In USA revenge pornography laws are enacted on a state level, therefore the laws differ from one another; some states treating revenge pornography as a misdemeanour, others treating it as a crime. Virginia was the first state, which has banned virtual revenge pornography. A bill to amend and re-enact § 18.2-386.2 of the Code of Virginia, relating to unlawful dissemination or sale of images of another, falsely created videographics or still images stipulates:

> Any person who, with the intent to coerce, harass, or intimidate, maliciously disseminates or sells any videographic or still image created by any means whatsoever, including a falsely created

> videographic or still image, that depicts another person who is totally nude, or in a state of undress so as to expose the genitals, pubic area, buttocks, or female breast, where such person knows or has reason to know that he is not licensed or authorized to disseminate or sell such videographic or still image is guilty of a Class 1 misdemeanour.

However, if a person uses services of an internet service provider, an electronic mail service provider, or any other information service, system, or access software provider that provides or enables computer access by multiple users to a computer server in committing acts prohibited under this section, such provider shall not be held responsible for violating this section for the content provided by another person. Virtual revenge pornography is included as "a falsely created videographic or still image" as such the current legislation in Virginia is completely appropriate to combat virtual revenge pornography. California on the other hand, has banned the distribution of maliciously deceptive audio and video content that misrepresents political candidates ahead of general elections, but there is no talk of virtual revenge pornography. There is currently no legislation on the federal level that effectively criminalizes revenge pornography or virtual revenge pornography. Even though the prosecution of virtual revenge pornography is possible under other computer crimes, e.g. unauthorized access or hacking, such prosecution may not result in a desirable outcome, as the laws do not focus on the true harm of sharing virtual revenge pornography. These state laws can only be used as an alternative option to prosecute virtual revenge pornography, but they are not ideal(Delfino, 2019, p. 920).

As in Europe and the US, the ideal statute would prohibit the online publication of virtual revenge pornography and would not require specific intent to harm the victim. The intent, *mens rea*, of the perpetrator should only cover the wilful dissemination of virtually created sexually explicit content. That is to say, where the perpetrator is aware that the individual depicted in the content did not consent to such sharing, nevertheless he shares it intentionally. The fair and proper legislation would not only punish the creators of such content but also other online circulators, when they participate in sharing such content knowingly that it was created without the consent of the victim and is now used to hurt the reputation or sexual integrity of the victim. The ideal revenge pornography statute would criminalize virtual and real revenge pornography videos. The potential hurdle for criminalization in the US is the First Amendment, which also protects the image "related to a matter of public interest, public concern, or related to a public figure who is intimately involved in the resolution of important public questions, or by reasons of his fame shapes events in areas of concern to society" (West, 2018 inHarris, 2018, p. 124). These limitations are unlikely to apply to most virtual revenge pornography, but they may be implicated if the statute covers public

figures whose images are published online without their consent (Harris, 2018, p. 124).

4. Conclusion

As it can be apparent from the findings of this article, virtual revenge pornography is not some dystopian idea from the future but a present-day threat and a legislative hurdle. The current technology is easily accessible, growing in prevalence and producing increasingly more realistic fakevideos. As a consequence, video content online cannot be taken at face value anymore.The days when fake videos were only used as a source of entertainment on TV shows or as Hollywood movie masterpieces are long gone. It would be unrealistic to state that current laws around the world effectively protect the victims of virtual revenge pornography. When it comes to the effort of the legislators to combat this phenomenon, it seems that the technology has an upper hand. The legislators lack the complex understanding of the technology behind it and therefore the ramifications seem unforeseeable. At present, it is impossible to talk about any clear-cut solution that would work. With the newest technologies, these videos are becoming more convincing, seamless and real, and can be effectively used to distort the truth, to manipulate and sow misinformation among voters in political campaigns.

A question at hand is the line between real life and fiction. How can the legal system, which cannot keep up with technology, effectively protect the integrity of an individual and society as a whole? Because of its complexity, it is becoming increasingly clearer that the virtual revenge pornographyphenomena cannot be effectively regulated on just one front line.While clear and precise legislation is most definitely needed, an important role in preventing the dissemination of such videos is also played by online platforms and in the end also by increasing the awareness of society, that creation of such videos is a serious offence that can deeply affect an individual, maybe even more than a real video. The law may forbid certain actions, however, at the endit is the social consciousness that matters more.

Since virtual revenge pornography is a relatively new cyber offence, the goal of the article was to present some new dilemmas that are arising in criminal law, as well as legislation of certain countries in order to show their readiness to prosecute virtual revenge pornography and similar digitally created digital content in the future. Poor definitions in the criminalcodes can have serious detrimental effects in legalpractice, resulting in unsuccessfulprosecutions of potential crimes. Precise criminal definition is a prerequisite for combating thisnew criminal offence in the future, which will only gain new dimensions (creation ofAI-doctored videos or photos forelection purposes, defrauding

purposes and pornography purposes). Legislators allover the world must therefore be prepared to deal with this new cybercrimephenomenon.

Bibliography

Ashcroft v. The Free Speech Coalition, 122 S. Ct. 1389 (2002).Retrieved from: https://www.courtlistener.com/opinion/118496/ashcroft-v-free-speech-coalition/.

Burris, A. (2014). Hell hath no fury like a woman porned: Revenge porn and the need for a federal nonconsensual pornography statute. Fla. L. Rev., 66, 2325.Retrieved from: http://www.floridalawreview.com/wp-content/uploads/11-Burris.pdf.

Byberg, J. (2012). Childless Child Porn-A 'Victimless' Crime? A Comparative Analysis of the Validity of the Current Restrictions in the United Kingdom and United States on Virtual Child Pornography in Relation to the Right to Free Speech. (July 20, 2012). Retrieved from: SSRN: https://ssrn.com/abstract=2114564 or http://dx.doi.org/10.2139/ssrn.2114564.

Chesney, B., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. Calif. L. Rev., 107, 1753.Retrieved from: https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=1640&context=faculty_scholarship.

Chesney, R., & Citron, D. (2019). Deepfakes and the new disinformation war: The coming age of post-truth geopolitics. Foreign Aff., 98, 147.Retrieved from: https://www.foreignaffairs.com/print/node/1123492.

Cisneros, D. (2002). Virtual Child Pornography on the Internet: A "Virtual" Victim? Duke Law & Technology Review, 1(1), 1-8.Retrieved from: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1060&context=dltr.

Citron, D. K., & Franks, M. A. (2014). Criminalizing Revenge Porn. Wake Forest Law Review, 49, 345-391.Retrieved from: https://digitalcommons.law.umaryland.edu/fac_pubs/1420/.

Clough, J. (2015). Principles of Cybercrime (second Ed.). Cambridge: Cambridge University Press. Retrieved from: http://202.166.170.213:8080/xmlui/bitstream/handle/123456789/3929/%20Principles%20of%20cybercrime.pdf?sequence=1&isAllowed=y.

Code pénal [French Penal Code]. French Republic, FRA-1992-L-62828 (2018). Retrieved from: http://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=62828.

Codice in materia di *protezionedeidatipersonali*, (Italian Data Protection Code). Italian Republic, Legislative Decree no. 101/2018 (2018).

Retrieved from: https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:decreto.legislativo:2003-06-30;196!vig=.

Criminal Justice Act. United Kingdom, Queen's most Excellent Majesty (2015).Retrieved from: http://www.legislation.gov.uk/ukpga/2015/2/introduction/enacted.

Deisinger, M. (2002). Kazenskizakonik s komentarjem, posebnidel[Slovenian Criminal Code with Commentary]. Ljubljana: GV Založba.

Delfino, R. A. (2019). Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act. Fordham L. Rev., 88, 887.Retrieved from: https://ir.lawnet.fordham.edu/flr/vol88/iss3/2.

Ellis G. E. (2019, July 24). New York's Revenge Porn Law Is a Flawed Step Forward. Wired. Retrieved from: https://www.wired.com/story/new-york-revenge-porn-law/.

Farokhmanesh, M. (2018). Is It Legal to Swap Someone's Face into Porn without Consent?. Verge. January, 30.Retrieved from: https://www.theverge.com/2018/1/30/16945494/deepfakes-porn-face-swap-legal.

Franks, M. A. (2013). Criminalizing revenge porn: Frequently asked questions. Retrieved from:https://ssrn.com/abstract=2337998 or http://dx.doi.org/10.2139/ssrn.2337998.

Franks, M. A. (2017). Revenge Porn Reform: A View from the Front Lines. Fla. L. Rev.69, 1251.Retrieved from: https://heinonline.org/HOL/LandingPage?handle=hein.journals/uflr69&div=43&id=&page=.

Franks, M. A., & Waldman, A. E. (2018). Sex, Lies, and Videotape: Deep Fakes and Free Speech Delusions. Md. L. Rev., 78, 892. Retrieved from: https://heinonline.org/HOL/LandingPage?handle=hein.journals/mllr78&div=34&id=&page=.

Gershgron D. (2018). Google Gave the World Powerful AI tools, and the world made porn with them, Quartz. Retrieved from: https://qz.com/1199850/google-gave-the-world-powerful-open-source-ai-tools-and-the-world-made-porn-with-them/.

Goudsmit, M. L. R. (2017). Revenge pornography: a conceptual analysis. Undressing a crime of disclosure (Master's thesis).Retrieved from: https://www.researchgate.net/publication/324360144_Revenge_pornography_A_conceptual_analysis_Undressing_a_crime_of_disclosure.

Hall, H. K. (2018). Deepfake Videos: When Seeing Isn't Believing. Cath. UJL & Tech, 27, 51.Retrieved from: https://heinonline.org/HOL/LandingPage?handle=hein.journals/cconsp27&div=6&id=&page=.

Harris, D. (2018). Deepfakes: False pornography is here and the law cannot protect you. Duke L. & Tech. Rev., 17, 99. Retrieved from: https://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1333&context=dltr.

HrvatskiKaznenizakon[Croatian Criminal Code]. Republic of Croatia, Croatian Gazette 118/18 (2018). Official translation, Croatia Ministry of Foreign and European Affairs. Retrieved from: http://www.mvep.hr/files/file/dokumenti/prevodenje/zakoni/kazneni-zakon-nn-125-11-eng.pdf

Hudson, D. L. (2002). Reflecting on the Virtual Child Porn Decision, 36 J. Marshall L. Rev. 211 (2002). The John Marshall Law Review, 36(1), 6.Retrieved from: https://heinonline.org/HOL/LandingPage?handle=hein.journals/jmlr36&div=14&id=&page=.

Jaishankar, K. (2018). Cyber Criminology as an Academic Discipline: History, Contribution and Impact. International Journal of Cyber Criminology, 12(1), 1-8. Retrieved from: http://www.cybercrimejournal.com/JaiEditorialVol12Issue1IJCC2018.pdf

Kamal, M., & Newman, W. J. (2016). Revenge Pornography: Mental Health Implications and Related Legislation, Journal of the American Academy of Psychiatry and the Law, 44(3), 359-367.Retrieved from: https://www.semanticscholar.org/paper/Revenge-Pornography%3A-Mental-Health-Implications-and-Kamal-Newman/9283a01263d26c34dfe2f7943ee18ea311a4a8da.

Kazenskizakonik, KZ-1 [Slovenian Criminal Code]. Republic of Slovenia, Uradni list RS 27/17 (2017). Retrieved from: http://www.pisrs.si/Pis.web/pregledPredpisa?id=ZAKO5050.

Ley Organica[Spanish Penal Code]. Kingdom of Spain, Jefaturadel Estado (2015). Retrieved from: https://www.boe.es/diario_boe/txt.php?id=BOE-A-2015-8167.

LOI n° 2016-1321 du 7 octobre 2016 pour uneRépubliquenumérique[Digital Republic Law]. French Republic, JORF n°0235 (2016). Retrieved from: https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000033202746&categorieLien=id.

Mills, L. (2002). Ashcroft v Sharpe: the virtual reality of child pornography. Child Abuse Research in South Africa, 3(2), 34-42.Retrieved from: https://journals.co.za/content/carsa/3/2/EJC24246.

Paul, B., & Linz, D. G. (2008). The effects of exposure to virtual child pornography on viewer cognitions and attitudes toward deviant sexual behavior. Communication Research, 35(1), 3-38.Retrieved from: https://journals.sagepub.com/doi/abs/10.1177/0093650207309359.

Pegg, S. (2018). A matter of privacy or abuse? Revenge porn in the law. Criminal Law Review, (7), 512-530.Retrieved from:http://irep.ntu.ac.uk/id/eprint/33944/.

Šepec, M. (2018).Kibernetskikriminal: Kaznivadejanja in kazenskopravnaanaliza[Cybercrime: Criminal Offences and Criminal Law Analysis]. Maribor: Law Faculty of University of Maribor.

Serbian criminal code, Official Gazette of RS, Nos. 85/2005, 88/2005, 107/2005 (2006). Translated by OSCE Mission to SaM, 2006. Retrieved from:https://www.osce.org/files/f/documents/5/2/18244.pdf.

Spivak, R. (2019). Deepfakes": The newest way to commit one of the oldest crimes. The Georgetown Law Technology Review, 3(2), 339-400. Retrieved from: https://georgetownlawtechreview.org/wp-content/uploads/2019/05/3.1-Spivak-pp-339-400.pdf.

Strafgesetzbuch – StGB[German Criminal Code]. Federal Republic of Germany, Federal Law Gazette I, p. 844 (2019), official translation. Retrieved from: https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html.

Virginia H.B. 2678, 2019 Session, An act to amend and reenact § 18.2-386.2, of the Code of Virginia, relating to unlawful dissemination or sale of images of another person. Retrieved from: https://www.mdpi.com/2075-471X/3/3/529.

Wall, D. S. (2015). The Internet as a conduit for criminal activity. Information technology and the criminal justice system, Pattavina, A., ed, 77-98.Retrieved from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=740626.