Studia Iuridica 93
ISSN 0137-4346; e-ISSN 2544-3135

DOI: https://doi.org/10.31338/2544-3135.si.2022-93.1

István Ambrus
Eötvös Loránd University, Faculty of Law, Department of Criminal Law, Hungary
Centre for Social Sciences, Institute for Legal Studies
e-mail: ambrus.istvan@ajk.elte.hu
ORCID: 0000-0001-6390-171X

THE NEW SEXUAL OFFENCES IN THE LIGHT OF DIGITALISATION

NOWE PRZESTĘPSTWA SEKSUALNE W ŚWIETLE DIGITALIZACJI

Abstract

Digitalisation has given rise to many new types of offences against sexual autonomy that previously either did not exist or at least were not so easily and quickly perpetrated.

The first of these is the category of deepfakes. The term "deep" refers to the deep learning, AI-based technology; "fake" denotes a manipulation, which, in summary, is the use of algorithms to manipulate images or video footage to make it possible to mount someone's face in a lifelike form on the footage – typically pornographic footage – that does not initially depict them. In practice, however, deepfakes are used not only in connection with pornographic content but often also to discredit political or business opponents.

Revenge porn usually involves publishing pornographic images of the victim by the former partner out of jealousy or revenge for the break-up of a relationship. Such images or videos may be of the (typically nude) victim himself or herself, a sexual act between the perpetrator and the victim, or may be manipulated images rather than real ones, where revenge pornography is combined with deepfakes.

Upskirting literally means "photographing under a skirt", which typically involves taking unauthorised pictures or videos of female victims' crotches. Of course, cameras existed before the advent of digitalisation, but it is only in the last decade or so that large numbers of people have a smartphone with the ability to take high-quality pictures of virtually every passer-by. Unfortunately, technological progress in this area has had a criminogenic effect, since it is easy to take such pictures or videos of an unsuspecting victim quickly and often unnoticed using a mobile phone.

Cyberflashing is the phenomenon of sending a picture or video of the offender's genitalia to the victim via a digital device without prior consent or agreement.

KEYWORDS

criminal law, cyberflashing, deepfake, revenge porn, upskirting

SŁOWA KLUCZOWE

prawo karne, przesyłanie zdjęć lub nagrań wideo, manipulowanie obrazami lub nagraniami wideo, zemsta porno, robienie nieautoryzowanych zdjęć

In this paper, I will present some of the new behaviours with a sexual dimension brought to life by the opportunities offered by digitalisation, which are considered dangerous to society and which are expected to appear soon (or have already appeared), thus posing a challenge from the point of view of law enforcement and legislation.

DEEPFAKE

The category *deepfake is* difficult to translate into other languages (like Hungarian). The term "deep" refers to the deep learning, AI-based technology; "fake" denotes a manipulation, and, in a nutshell, it refers to image or video footage manipulated by algorithms to make a lifelike montage of someone's face on a shot – typically a pornographic shot – that does not originally depict it.[1] In practice, however, deepfakes are not only used in connection with pornographic content but often also , for example, to discredit political or business opponents. In the USA, Article 18 of the Code of Virginia has since 2019 made it a crime, the

[1] R. A. Delfino, *Pornographic deepfakes: The case for federal criminalization of revenge porn's next tragic Act*, "Fordham Law Review" 2019, Vol. 88, No. 3, p. 892–893.

so-called revenge pornography offence, to make a person appear to be a person in pornographic material for sexual purposes (deepfake pornography, see also the next point). The first state to make deepfake a crime for political manipulation was Texas. The Texas Senate Bill 751, of 1 September 2019, punishes with imprisonment for up to one year or a fine of up to $4,000 anyone who makes a deceptive video with the intent or result of influencing the outcome of an election. Finally, California's comprehensive legislation of 11 October 2019, which includes both deepfake manipulation of political campaigns (Assembly Bill No. 730) and pornographic manipulation of recordings (Assembly Bill No. 602), is worthy of note.

In Hungarian criminal law, using deepfakes may constitute, above all, the crime of misuse of personal data. The reason for this is that Article 3(3b) of the Info Act considers *biometric data* as special personal data, which is, for example, personal data concerning the physical characteristics of a natural person that allows for or confirms unique identification of a natural person, such as a *facial image*, so that if someone's facial image is added to the body of a person in a pornographic film, this act can be considered as unauthorised personal data processing, provided of course this happens without his or her consent. And if it is done for profit or to cause substantial damage to his/her interests, the abuse of personal data under Article 219 (1) *(a)* of Act C of 2012 on the Hungarian Criminal Code (hereinafter: the Criminal Code) may be deemed to have been committed. In a relationship context, the result of substantial damage to interests may of course be of more practical significance. This could be the case if someone suffers a disadvantage in his/her workplace or private life due to the publication of a fake photo (e.g. dismissal, disruption of a new relationship, etc.). Kinga Sorbán also raises the possibility of harassment in the context of deepfakes, but this could only be the case if the perpetrator regularly sends the manipulated image to the victim him- or herself.[2] If, on the other hand, the transmission is to another person, harassment can be excluded. However, the offences of blackmail or making a false image or sound recording capable of defamation (Article 226/A of the Criminal Code) and publication thereof (Article 226/B of the Criminal Code) may arise.

The category of deepfake does not, in my opinion, carry an additional danger to society that would require the creation of a separate factual situation, because if significant harm to the interests can be established, the act, as we have seen, can be classified as misuse of personal data without any concerns. If such a result cannot be established, then, pursuant to Section 2:43 *(g)* of the Civil Code, the infringement of the right to the likeness may still be subject to a so-called likeness suit pursuant to Section 502 (1) of Act CXXX of 2012 on the Civil Procedure Act . In view of these circumstances, a further expansion of the criminal threat in this area is not recommended.

[2] K. Sorbán, *A bosszúpornó és deepfake pornográfia büntetőjogi fenyegetettségének szükségességéről*, "Belügyi Szemle" 2020, No. 10, p. 99–100.

REVENGE PORN

Revenge pornography usually involves the publication of pornographic images of the victim by the ex-partner out of jealousy and revenge for the break-up of a relationship.[3] Such images or videos may be of the (typically nude) victim alone, of a sexual act between the perpetrator and the victim, or may be manipulated rather than real, where revenge pornography is combined with deepfakes. In the US literature, revenge pornography is understood as a subset of a broader concept, *nonconsensual pornography* (NCP). This category covers the distribution of private, explicit images of the victim without the consent of the victim.[4]

Revenge pornography has been criminalised in some US states since 2000 (first in West Virginia and then in New Jersey), and by 2019, 41 states had already criminalised it.[5] In addition, as early as 2014, there was already a position in the literature calling for federal regulation.[6] 2012 saw a serious case of a victim who committed suicide because of pornographic images of her that had been made public.[7] As an example of a national provision, Section 245 of the New York State Penal Law (NY Penal Law), which was adopted in the US in December 2008, as of 2019 makes it a criminal offence to intentionally publish or publish a still or video image of another person if the image does not show the victim wearing clothing or if the image is of a sexually explicit sex act or of the victim performing a sex act. To establish the elements of the offence, the offender must intend to cause emotional, material or physical harm to the victim. In Ohio, the knowing disclosure of a nude or sexually explicit image of a person performing a sexual act is sufficient to constitute the offence.[8]

In Australia, 2018 saw the federal regulation of revenge pornography. The Enhancing Online Safety Act added the offence of non-consensual sharing of intimate images to the Criminal Code Act of 1995, with a maximum penalty of up to 7 years' imprisonment.

---

[3] J. S. Sales, J. A. Magaldi, *Deconstructing the statutory landscape of "revenge Porn": An evaluation of the elements that Make an effective nonconsensual pornography statute*, "American Criminal Law Review" 2020, No. 4, p. 1501.

[4] B. Armesto-Larson, *Nonconsensual pornography: Criminal law solutions to a worldwide problem*, "Oregon Review of International Law" 2020, No. 1, p. 181.

[5] https://www.nbcnews.com/news/us-news/new-york-poised-join-41-other-states-criminalizing-revenge-porn-n977871 (accessed 29.03.2021).

[6] See T. Linkous, *It's time for revenge porn to get a taste of its own medicine: An argument for the federal criminalization of revenge porn*, "Richmond Journal of Law & Technology" 2014, No. 4. pp. 1–39.

[7] J. S. Sales, J. A. Magaldi, *Deconstructing the statutory landscape...*, p. 1508.

[8] Ohio Rev. Code Ann. § 2917.211

In England and Wales, this action was criminalised in April 2015. Here, posting images and videos of explicit sexuality on the Internet is a criminal offence (Criminal Justice and Courts Bill), punishable by up to 2 years' imprisonment.[9]

Revenge pornography, like deepfakes, may primarily constitute a misuse of personal data, and if the perpetrator threatens the victim, for example, to make their joint photos public if he or she does not have sexual relations with him or her again, sexual coercion (Section 195 of the Penal Code) may be established. The offence of extortion may also be involved in the case of unjustified claims to property. Harassment may also be established, albeit the requirement of regularity means that it is a classification with less practical relevance.

In connection with this act, *de lege ferenda*, I consider it more conceivable to regulate it as a *sui generis* criminal offence. The reason for this is that revenge porn also infringes an additional legal subject matter that neither the misuse of personal data nor any other of the aforementioned offences can fully protect. This legal object is a sub-aspect of the right to sexual self-determination, namely the right to decide for oneself, in relation to pornographic recordings made with the consent of the victim, whether and to what extent to make such recordings public. Thus, in the area of offences against sexual freedom and sexual morality, for example, the offence of *unauthorised disclosure of pornographic material* could be regulated in Article 205/A of the Criminal Code, which would be committed by anyone who makes available or discloses pornographic material of another person to a third party without the consent of that person, unless a more serious offence is committed. These offences could be regulated as misdemeanours punishable by up to two years' imprisonment, and would be subject to the lodging of a private prosecution.

UPSKIRTING

Upskirting typically involves taking unauthorised pictures or videos of female victims' crotches.[10] Of course, cameras existed before the advent of digitalisation, but it is only in the last decade or so that large numbers of people have a smartphone with the ability to take high-quality pictures. Unfortunately, technological progress in this area has had a criminogenic effect, as it is easy to take such pictures or videos of an unsuspecting victim quickly and often unnoticed.

[9] M. Yar, J. Drew, *Image-based abuse, non-consensual pornography, revenge porn: A study of criminalization and crime prevention in Australia and England & Wales*, "International Journal of Cyber Criminology" 2019, No. 2, pp. 578–594.

[10] See J. T. Marvin, *Without a bright-line on the green line: How Commonwealth v. Robertson failed to criminalize upskirt photography*, "New England Law Review" 2015, No. 1, p. 124.