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.

As regards the historical aspects, it is worth mentioning that this act has a very long history, so that even in Roman law there was already a case of *adtemptata pudicitia*, which meant the seduction of unmarried girls or married women in public places.

Scotland was the first country in the UK to make upskirting a separate offence. Section 9 of the Sexual Offences (Scotland) Act, which came into force in 2010, penalises so-called voyeurism, which is essentially the covert observation of the sexual activity of another person. However, subsection 4B of that Act makes it a separate offence to take a photograph of a victim's genitals or buttocks while the victim is clothed, without the consent of the victim (or a reasonable presumption of consent), regardless of whether the victim is wearing underwear.[11]

Subsequently, following an incident involving Gina Martin in Hyde Park, London, in July 2017,[12] the legislature of England and Wales had to take action, which finally transpired in April 2019, when upskirting was added to the Sexual Offences Act 2003, through the Voyeurism (Offences) Act 2019. Thus, section 67A(2) of this Act, like the Scottish legislation, makes it an offence to take a photograph of the groin, under clothing, without permission. The penalty is imprisonment for up to two years.

The legislation in the US was triggered by an incident on 11 August 2010, when Michael Robertson, travelling on a train in Boston, used his mobile phone to take a photo up a woman's skirt. In *Commonwealth v. Robertson*,[13] the Massachusetts Supreme Judicial Court ruled that upskirting was not punishable under Massachusetts General Law 272, Chapter 105(b), since that statute criminalised, at the time of the offence, anyone who videotaped or observed, through a digital device, a person who was partially or fully nude. However, in the case at hand, the victim was wearing underwear, and the court did not find that she was partially naked.[14] In a typical development, the ruling caused such a public outcry that the national legislature amended the relevant legislation 2 days after the judgment was delivered to make upskirting punishable also in relation to a victim wearing underwear.[15]

---

[11] On the Scotish regulation see G. Lipschitz, *Can the issues of cyberbullying and sexting be addressed by legislation alone? A critical analysis of the current legislative measures and societal measures needed to protect our youth in the digital realm*, "Edinburgh Student Law Review" 2020, No. 1, p. 71.

[12] See https://www.dailymail.co.uk/news/article-6602107/Upskirting-victim-tells-horrifying-moment-realised-man-took-picture-skirt.html (accessed 15.05.2021).

[13] N.E.3d 522 (Mass. 2014).

[14] See J. L. Stathi, *Criminal law – when upskirting was not illegal: A court-ordered legislative fix – Commonwealth v. Robertson, 5 N.E.3D 522 (Mass. 2014)*, "Suffolk Journal of Trial & Appellate Advocacy" 2015, No. 1, pp. 333–343.

[15] K. Hong, *A new mens rea for rape: More convictions and less punishment*, "American Criminal Law Review" 2018, No. 2, p. 273.

In the German legal literature, Gloria Berghäuser has examined whether upskirting can be covered by a provision of the German Criminal Code. She sees this area as unregulated, but draws attention to the fact that in the event of criminalisation, it is essential to consider what interests the legislator would like to protect with the new offence, what conduct should be punished and whether it would not be sufficient to create a liability for the offence.[16] Eventually, however, the German legislator has made this offence punishable recently (StGB § 184k).

Finally, to return to a US source for a moment, Michael Whiteman analyses the impact of technological developments on law. He cites the examples of upskirting and Bitcoin, and uses these two typical developments in digitalisation to show that the *rule of law* doctrine does not allow courts to expand the interpretation of old criminal law, but instead requires the legislature to act where digital changes create loopholes that cannot be penalised.[17]

With this in mind, I would like to draw the reader's attention to the fact that the criminalisation of upskirting should also be considered by future domestic legislation in Hungary. It cannot be regarded as a sexual act [Section 459(1) (27) of the Criminal Code], because that necessarily requires physical contact between the perpetrator and the victim, so that the establishment of more serious sexual offences (such as sexual violence or sexual coercion) is certainly out of the question. A form of indecent assault (Article 205 of the Penal Code) may be investigated. However, in order for Article 205(1) of the Penal Code to be applicable, it is necessary that the perpetrator, motivated by sexual desire, exhibits him- or herself in a lewd manner to others. A subsidiary offence under Paragraph 205(2) of the Penal Code may only be committed by a person over the age of 18 against a victim under the age of 14, also motivated by sexual desire, by engaging in indecent conduct. However, the taking of photographs is not considered to be indecent assault. Thus, the finding of these offences can in principle be excluded in the context of upskirting. In the context of indecent assault under Section 205(3) of the Criminal Code, the law punishes, according to the relevant ministerial reasoning, conduct which is not seriously indecent and which therefore cannot amount to sexual violence or sexual coercion. The commentary literature, which refers to this type of offence as objective indecency, includes minor indecent conduct requiring physical interaction (for example, holding the victim's breasts or buttocks against his or her will, kissing the victim).[18] In other words, actions which could have been con-

[16] G. Berghäuser, *Upskirting und ähnliche Verhaltensweisen Unbefugte fotografische oder filmische Aufnahmen unter der Oberbekleidung*, "Zeitschrift für Internationale Strafrechtsdogmatik" 2019, No. 10, p. 475.

[17] M. Whiteman, *Upskirting, BitCoin, and crime, oh my: Judicial resistance to apply old laws to new crimes – what is a legislature to do?*, "Indiana Law Journal Supplement" 2020, No. 5, pp. 72–78.

[18] Zs. Szomora, *A nemi élet szabadsága és a nemi erkölcs elleni bűncselekmények*, (in:) Karsai K. (ed.), *Nagykommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez [online]*, Budapest 2019.

sidered as defamatory acts under the 1978 Criminal Code [Section 180(2) of the 1978 Criminal Code, Section 227(2) of the 1978 Criminal Code]. This view must be clearly agreed with, and the interpretation of the law cannot be extended in the direction of upskirting, if only because Section 205(3) of the Criminal Code also requires the commission of indecent behaviour (which violates the human dignity of the victim). This form of indecency can be established without any concerns, as in a 2017 case where minors aged between 14 and 16 years old behaved indecently towards 9 women in the vicinity of the Parliament, which they recorded with their mobile phones.[19]

As mentioned above, harassment under Section 222(1) of the Criminal Code would only be established in the case of regular (or persistent) misconduct, and upskirting is therefore not typically punishable under this provision. It could be argued that defamation could be considered to fall under the category of "other such acts" capable of damaging honour. However, due to the presumable absence of the situational elements described in Section 227(1) *(a)* or *(b)* of the Criminal Code, in practice only the offence of defamation under Section 180(1) II of Act II of 2012 on Regulatory Offences (hereinafter: Szabs. tv.) applies.

In view of the above, and also in the light of the considerations cited, it must first of all be clarified whether there is a legal right which is attacked by upskirting. In my view, such a right is an aspect of the right of sexual self-determination that no recordings of the victim's intimate parts of his body may be made or disclosed against his or her will. The higher degree of danger to society and general prevention may also require prosecution as a criminal offence instead of liability for offences. Hence my *de lege ferenda* proposal would comprise:

– a misdemeanour of making an unauthorised intimate recording, with a person who makes an indecent recording of another person without his or her consent punishable by up to 1 year's imprisonment (future Section 205/B of the Criminal Code),

– a misdemeanour of disclosure of an unauthorised intimate recording, with a person who makes available a lewd recording of another person without his or her consent punishable with up to 2 years' imprisonment (future Section 205/C of the Criminal Code).

Finally, in order to avoid legal uncertainty, it would be useful to define the concept of intimate recording at the end of the § in an interpretative provision. This should include video, film and photographic recordings in which the perpetrator depicts or attempts to depict sexuality with indecent frankness. The latter, as an auxiliary measure, would also make it possible to include a recording of the victim wearing underwear in the offence.

I should note here that in April 2019, an amendment to the law was also submitted in Hungary, which would have criminalised certain cases of upskirting

[19] https://index.hu/belfold/2019/04/10/csoportosan_szemeremserto_fiatalok/ (accessed 15.05.2021).

under the headings of "making a picture with sexual content or other degrading content suitable for defamation" or "publishing a picture with sexual content or other degrading content suitable for defamation".[20] The call for penalisation may be the right direction, but in my opinion, these facts should be explicitly regulated in the sexual chapter of the Criminal Code, given that their primary legal object is sexual self-determination, not human dignity.

## CYBERFLASHING

*Cyberflashing* is the sending of a picture or video of the genitalia of the perpetrator, typically male, to the victim via a digital device without prior consent or agreement.[21] The transmission of unsolicited sexual content in this form can therefore be considered the inverse of upskirting.

According to empirical research by a law student at ELTE-AJK, 2/3 of more than 200 respondents have received unsolicited sexual messages, usually through Messenger, Instagram and Tinder (the latter being a dating app). The reaction of the respondents was mostly negative, many blocked the sender and the majority were disturbed by the viewing of such a message. According to the relevant questionnaire, almost 80% of respondents would like to see cyberflashing made a criminal offence.[22]

McGylnn and Johnson, who have examined the issue in detail in the recent Anglo-Saxon literature, point out that the spread of cyberflashing was largely catalysed by the Covid19 pandemic. The authors focus on the criminal law aspects of cyberflashing in the context of harassment, concluding that such acts do not generally fall neatly within the Anglo-Saxon definition of harassment. They then go on to examine in detail three related regimes, namely that of Singapore, the US State of Texas and Scotland.

Since January 2020, cyberflashing is a *sui generis* offence in Singapore, committed by anyone who intentionally sends images of his or her own or another person's genitals to another person for the purpose of the victim seeing the images, whereby the offender seeks to gratify his or her sexual desire or to humiliate the victim. This offence is punishable by up to one year's imprisonment.

As of September 2019, Texas also regulates this offence as a separate offence of unlawful electronic transmission of sexually explicit visual material. The regulation is likewise quite broad, although, interestingly, the offence can only be

[20] T/5869. Parlex azonosító: 1NSIHI1O0001.

[21] C. McGlynn, K. Johnson, *Criminalising cyberflashing: Options for law reform*, "The Journal of Criminal Law" 2020, No. 3. p. 172.

[22] Bodori K., *Criminal law-related issues to cyberflashing: Report*, Budapest 2021.

committed by a man. The penalty is a fine of up to $500.[23] Here the authors refer to the legislation in California, where the FLASH Act (Forbid Lewd Activity and Sexual Harassment, 2020), which came into force in February 2020, also imposes a fine of up to $500 (or$1,000 for repeat offences) on anyone who knowingly transmits indecent or explicit sexual content to another person via electronic means.

Scotland's criminal law – which, as we have seen, also pioneered the criminalisation of upskirting – criminalised the act of forcing someone to view a sexual image as early as 2009. The cited authors point out that, although this legislation was not introduced at the time to combat cyberflashing, case law has extended its application to the new phenomenon. Very severe prison sentences of up to 10 years are possible for these offences.[24]

Cyberflashing, as the author cited above suggests, could also give rise to a finding of harassment in Hungary. However, as we have seen, the existence of regularity (or permanence) as a mode of commission is elementary for the establishment of this offence under Article 222 (1) of the Criminal Code, and consequently a single sending of an image cannot become a factual element. Harassment under Article 222 (2) *(b)* of the Criminal Code, which may be committed by making a false pretence of an event directly endangering the life or physical integrity of another, although not requiring regularity, would only be established in very extreme cases of cyberflashing – for example, if the background of the image of a genital organ indicates a threat of a sexual act of a sadomasochistic nature.

Transmission of child pornography can be charged if the person in the picture is under 18. It should be stressed here that a minor who transmits an image of himself or herself to another person may also be a perpetrator. In addition, while a person who receives a photograph which he or she does not want to receive does not commit the offence of obtaining within the meaning of Article 204(1) *(a)* (I) of the Criminal Code, later, if he or she does not delete the recording because of his or her indifference, the *tart* turn may become a factual element, except of course if the offender regards the recording solely as evidence to be used in criminal proceedings and does not delete it for that reason.

All the problems that have been raised in relation to the ascertainability of sexual offences in the context of upskirting also arise as dilemmas in cyberflashing. The phrase "displaying oneself [...] before another [...]" [Article 205(1) of the Criminal Code] can be applied to offline offences. In my view, online, the offender can only be considered to have committed the offence if he or she does not simply send the victim an unsolicited, previously taken picture of his or her genitals (since he or she is then not actually "showing himself" but only the picture), but

[23] See B. C. Miller, *Fact or phallus? Considering the consitutionality of Texas's cyber-flashing law under the T=true threat doctrine*, "Texas A&M Law Review" 2021, No. 2, pp. 423–449.

[24] C. McGlynn, K. Johnson, *Criminalising cyberflashing...*, pp. 181–184.

if, for example, he or she initiates a live broadcast on Facebook and then, when the unsuspecting victim answers the call, immediately shows his or her genitals to the victim with the help of a camera. As we have seen, the prevailing interpretation of the phrase "engages in indecent behaviour towards another person which offends the human dignity of the victim" is that it presupposes physical contact. An interpretation could of course be envisaged which would include the sending of a picture of the genital organ to another person in the scope of the "indecent conduct" described in the offence of indecent assault under Article 205(3) of the Criminal Code. However, Article 28(2) of the Fundamental Law provides that "[i]n determining the purpose of legislation, the preamble to the legislation or the grounds for the proposal to enact or amend the legislation shall be taken into account in the first instance". The Ministerial Explanatory Memorandum to the Criminal Code expressly requires physical contact between the perpetrator and the victim in relation to Article 205(3) of the Criminal Code, and a solution which extends the scope of criminal liability to cover indecent acts without physical contact would therefore be contrary to the principle of legality.

As with upskirting, a finding of ancillary defamation may be raised, but, in the absence of a situational element, in practice at most in the form of liability for a misdemeanour.

What may also arise from the Szabs. tv. is the *violation of public morals* (Szabs. tv. Section 192), which is committed by anyone who in a public place, public space or a means of public transport engages in conduct contrary to public morals. Implementation in the digital space could be included in the concept of an offence against public morals committed in a public place, provided that the offence committed by means of an information system can be interpreted as having been committed in a public place without any concerns. According to Section 29(2) *(b)* of the Szabs. tv, a public place is a place open to the public and not considered to be a public space. A picture sent in a private messenger message cannot therefore be considered to have been transmitted in a public place. However, posting in a meeting that is open to everyone – for example, accessible with a link provided in advance, not as a closed conference on Zoom, MS Teams, etc. – may already give rise to this infringement. However, this also presupposes that the term "place" is not only understood in its conventional sense, but also includes virtual space, which, in the absence of an explicit legislative intention to this effect, could again raise problems of legality.

On this basis, cyberflashing would require *de lege ferenda* regulation. This could be done, on the one hand, by creating an interpretative provision to the offence of indecent exposure that would allow the offence to be established between absent parties, i.e. when the offender sends an indecent video to the victim via a digital device. On the other hand, it would of course be possible to envisage a *sui generis* definition of the offence, for example by drawing on the Singapore or Texas rules. In the latter case, it would make sense to regulate this

offence as a crime against sexual freedom and sexual morality, given the sexual nature of its primary legal object.

In drafting the new legislation, care should be taken to ensure that the scope of criminal liability does not become indiscriminate and does not risk gender discrimination, so that it could be stipulated that the offence should be punishable only by the transmission of a picture of the offender's own body. Otherwise, even the transmission to another person of any pornographic image downloaded from the Internet would constitute a criminal offence, which would still only be punishable by the offence of harassment if it is committed on a regular basis. It may be a question of whether the offence should be established only in the case of an image or video of a genital area or whether it should also be established by means of other images of sensitive parts of the body. Almost all the regulations referred to have emphasised the requirement of intent, which I believe should be adopted, so that if a person carelessly positions him- or herself in front of the camera in such a way that his uncovered genitals – which the perpetrator is not aware of because of the angle of the camera – are in fact visible to the other party, this act, because of the careless nature of the recording and transmission, would not constitute an offence.

The scope of criminal liability cannot be limited to male perpetrators, as under gender equality, an unsolicited pornographic recording can violate anyone's right to unhindered exercise of sexual self-determination, regardless of gender.

Another important issue to be examined is the problem of consent, which may not only be given expressly and in advance, but also implied or may even be subsequent consent, depending on the circumstances. In the case of a long-standing relationship, implied consent may also be recognised on the basis of established practice. It would be worthwhile to regulate the offence as a misdemeanour to be prosecuted on private initiative.

## CONCLUSION

At the end of my study, I emphasise that digitalisation poses new dangers for sexual self-determination that we have not been encountered before. Thus, for instance, taking or sending unsolicited pictures and falsifying them are now an everyday problem. With this in mind, it is worthwhile for the legislation to give quick and appropriate answers to the problems arising in this area.

## REFERENCES

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

Berghäuser G., *Upskirting und ähnliche Verhaltensweisen Unbefugte fotografische oder filmische Aufnahmen unter der Oberbekleidung*, "Zeitschrift für Internationale Strafrechtsdogmatik" 2019, No. 10

Bodori K., *Criminal law-related issues to cyberflashing: Report*, Budapest 2021

Delfino R. A., *Pornographic deepfakes: The case for federal criminalization of revenge porn's next tragic act*, "Fordham Law Review" 2019, No. 3

Hong K., *A new mens rea for rape: More convictions and less punishment*, "American Criminal Law Review" 2018, No. 2

Linkous T., *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

Lipschitz G., *Can the issues of cyberbullying and sexting be addressed by legislation alone? A critical analysis of the current legislative measures and societal measures needed to protect our youth in the digital realm*, "Edinburgh Student Law Review" 2020, No. 1

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

McGlynn C., Johnson K., *Criminalising cyberflashing: Options for law reform*, "The Journal of Criminal Law" 2020, No. 3

Miller B. C., *Fact or phallus? Considering the consitutionality of Texas's cyber-flashing law under the true threat doctrine*, "Texas A&M Law Review" 2021, No. 2

Sales J. S., Magaldi J. A., 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

Sorbán K., *A bosszúpornó és deepfake pornográfia büntetőjogi fenyegetettségének szükségességéről*, "Belügyi Szemle" 2020, No. 10

Stathi J. L., *Criminal law – when upskirting was not illegal: A court-ordered legislative fix – Commonwealth v. Robertson, 5 N.E.3D 522 (Mass. 2014)*, "Suffolk Journal of Trial & Appellate Advocacy" 2015, No. 1

Szomora Zs., *A nemi élet szabadsága és a nemi erkölcs elleni bűncselekmények*, (in:) Karsai K. (ed.), *Nagykommentár a Büntető Törvénykönyvről szóló 2012. évi C. törvényhez*, Budapest 2019

Whiteman M., *Upskirting, BitCoin, and crime, oh my: Judicial resistance to apply old laws to new crimes – what is a legislature to do?*, "Indiana Law Journal Supplement" 2020, No. 5

Yar M., Drew J., *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