Dr. Matthew Hall,

Associate Professor, Department of Psychology, Faculty of Arts & Humanities, BUE

Prof. Andreas Pester,

Faculty of Informatics and Computer Science, BUE

Dr. Alex Atanasov,

Assistant Professor, Faculty of Law, BUE

AI Threats to Women's Rights: Implications and Legislations

Correspondence:

Matthew Hall, Associate Professor, Department of Psychology, Faculty of Arts & Humanities, The British University in Egypt

DOI: https://doi.org/10.54873/jolets.v2i2.86

E-mail: Matthew.Hall@bue.edu.eg - Andreas.Pester@bue.edu.eg - Alex.Atanasov@bue.edu.eg

Citation:

Matthew Hall, Andreas Pester & Alex Atanasov, AI Threats to Women's Rights: Implications & Legislations, Paper submitted to the International Human Rights Conference on « Climate Justice, Human Trafficking, and Social Media & AI Regulation», organized by the Faculty of Law at British University in Egypt on August 28th 2022, Journal of Law and Emerging Technology, Volume 2, Issue 2, October 2022, p.51-88

AI Threats to Women's Rights:Implications and Legislations

Dr. Matthew Hall, Prof. Andreas Pester, Dr. Alex Atanasov

Abstract

The last few decades have seen a remarkable increase in the accessibility and capabilities of technologies using artificial intelligence, augmented, virtual, and mixed reality technologies, which allow users to create new virtual digital worlds, or generate unseen text, images, videos and sound. However, these new spaces have also provided new opportunities to use such technologies to harm women. This article tackles the threat of AI technologies to women's rights. First, we introduce the deepfake pornography technology based on AI. Second, we expose the gaps in the international legal order governing women's rights against threats posed by those technologies. Then, we provide three examples for domestic/regional legal frameworks which address AI threats to women's rights. These include regulations enacted in some US states, the UK's pending legislation and a proposal of a European Union law. We highlight the different challenges facing the creation and implementation of those laws. We address the different options for holding someone accountable for violations of women's rights through the Al technologies. We pinpoint the existence of gaps and weaknesses in contemporary legislations addressing Al threats to women's rights. Still we commend the efforts of the above leading jurisdictions that have brought developments in this important subject. Finally, we propose a way to identify the legally responsible entity in order to avoid the socially undesirable behavior that comes from deepfake pornography

Keywords: Women's rights; AI technologies; legislation; deepfake pornography

تهديد الذكاء الاصطناعي لحقوق المرأة: التداعيات والتشريعات

د. ماثيو هول، أ.د أندرياس بيستر، د. أليكس أتاناسوف

الملخص:

شهدت العقود القليلة الماضية زيادة ملحوظة في إمكانية الوصول إلى تقنيات استخدام الذكاء الاصطناعي، وتقنيات الواقع المعزز والافتراضي والمختلط وقدراتها، والتي تسمح للمستخدمين بإنشاء عوالم رقمية افتراضية جديدة، أو إنشاء نصوص وصور ومقاطع فيديو وصوت غير مرئية. ومع ذلك، فقد أتاح هذا الواقع الجديد أيضًا فرصًا جديدة لاستخدام هذه التقنيات لإيذاء المرأة.

ومن هنا يعالج هذا البحث تهديد تقنيات الذكاء الاصطناعي لحقوق المرأة. أولاً، نقدم تقنية التزييف العميق الإباحية القائمة على الذكاء الاصطناعي. ثانيا، نكشف الثغرات في النظام القانوني الدولي الذى يحكم حقوق المرأة ضد التهديدات التي تشكلها تلك التكنولوجيات. ثم نقدم ثلاثة أمثلة للأطر القانونية المحلية/ الإقليمية التي تعالج تهديدات الذكاء الاصطناعي لحقوق المرأة. ويشمل ذلك اللوائح التي تم سنها في بعض الولايات الأمريكية، والتشريع المنتظر في المملكة المتحدة واقتراح قانون الاتحاد الأوروبي. ونسلط الضوء على التحديات المختلفة التي تواجه وضع تلك القوانين وتنفيذها. كما نتناول الخيارات المختلفة لمحاسبة شخص ما على انتهاكات حقوق المرأة من خلال تقنيات الذكاء الاصطناعي.

ويشير البحث إلى وجود ثغرات ونقاط ضعف في التشريعات المعاصرة التي تعالج التهديدات التي تتعرض لها حقوق المرأة. وما زلنا نشيد بجهود الولايات القضائية الرئيسية التي أحدثت تطورات في هذا الموضوع الهام. أخيرًا، نقترح طريقة لتحديد الكيان المسئول قانونًا من أجل تجنب السلوك غير المرغوب فيه اجتماعيًا والذى يأتي من المواد الإباحية المُنتَجة عبر تقنيّة التزييف العميق .

الكلمات الرئيسية: حقوق المرأة، الذكاء الاصطناعي، التشريعات، المواد الإباحية المُنتَجة عبر تقنيّة التزييف العميق.

Introduction

Long gone are the days when existing in computer-generated virtual spaces was the subject of science fiction. Today, people can enter a multiplicity of virtual spaces to play games, enhance sports performance, learn to fly an airplane, practice complex surgical procedures, have immersive teaching experiences, try on clothing and footwear, buy virtual only items such as art, designer clothing, and real estate, and many others, including living a virtual second life (Bailenson, 2018). Market research organization Statistica (2021), estimates that market for such modern technologies will reach $300 billion by 2024, with an estimated 1.7 billion users worldwide. However, growth is likely to be uneven, favoring the more developed nations and regions who continue to have greater accessibility to technology and provide the digital literacy to us. (UN-Habitat, 2021).

Many of these virtual spaces integrate a range of modern immersive technologies. For example, artificial intelligence (AI), are machine learning algorithms in computer and robots that are programmed to simulate some human thinking processes (e.g., problem solving) (Pester et al., 2020). Unlike AI augmented reality (AR) software allows virtual objects (e.g., furniture, clothing) to be superimposed on the real world (e.g., images of a person's home) (Azuma, 1997), whereas virtual reality (VR) software immerses the user into a computer-generated artificial world (Carmigniani et al., 2011, p. 342). Mixed reality (MR) software on the other hand combines AR and VR to allow a person to experience a real environment shared with virtual objects and people (e.g., holograms) (Holz et al., 2011). If, or when, synthetic reality (SR) technologies are available, they will go one step further combining AI and MR, so that user actions and/or inputs will be anticipated in those virtual worlds (Castronova, 2008). The combination of all these technologies (and others) are what has become known as the 'metaverse' (Sparkes, 2021). That

is, a digital environment, or parallel virtual universe, that resembles, and coexists alongside people's own worlds and realities (Ramesh et al., 2022).

But whilst these modern technologies provide many benefits such as enhanced communications and the compression of space and time that can increase, for example, the delivery of health services (Hauer, 2022), education (Hilliker, 2022), and business (Farshid et al., 2018), they have also become increasingly used to harm women (Bailey and Burkell, 2021; Hall, Hearn and Lewis, 2022; Henry and Powell, 2014) such as the report of women's avatars being raped in VR (Oppenheim, 2022). Whilst both women and men can experience technology-facilitated abuses and violations, women are more likely to be targeted, with more intense abuse that is gender specific and sexualized (European Institute for Gender Equality, 2022). One particular insidious abuse of modern technologies is deepfake pornography.

Drawing on our research in AI and other emerging, modern, and advanced technologies noted above (Pester et al., 2020) and their abuses and violations against women (Hall, Hearn and Lewis, 2022), we explore deepfake pornography and its impacts and motives, considering the existing legal solutions and where there are gaps, highlighting the socio-legal implications. Our aim in doing so is not just to raise awareness of how these technologies can harm but also to provide a knowledge base for shaping socio-cultural-legal research that can inform policy-makers, legislators, designers and developers of new technologies, and for those professionals working with victim-survivors and perpetrator reeducation programs.

Deepfake pornography

Most AI is developed to be task specific such as in facial recognition, trading bots, and self-driving cars. However, a more developed subset of AI is developed for deep learning so that it operates similarly to the human brain with algorithms being able to identify patterns and classify various types of

information in real time as it is received. In this sense, AI can 'make decisions. For example, in deepfake technologies algorithms can make classifications of people's facial and bodily features on their own rather than requiring someone to manually inputted those classifications (Ajder et al., 2019). Deepfakes rely on large sets of data samples that can be analyzed by neural networks to learn to mimic people's facial expressions, body movements, mannerisms, voice and so on (Westerlund, 2019).

Where once deepfake technologies were largely accessible only to experts in specialized industries such as film production and criminal forensics, with the launch of programs like FaceApp2, it has become relatively easy for almost anyone with a basic level of IT knowledge and internet access to take someone else's online image, video, and voice, to create convincing deepfakes (Öhman, 2020). The ability of a wider number of people capable of using deepfake technologies has raised concerns about their abuses in the distribution of political disinformation, blackmailing, 'sockpuppeting'(1) and pornography (Citron and Chesney, 2018), and deepfake pornography (Franks, 2017).

The term 'deepfake' is a portmanteau of 'deep learning' and 'fake' and was apparently coined by a Reddit user with the same pseudonym in 2017 when they used AI to manipulate pornographic images (Maddocks, 2020). More than 90% of deepfake pornography is of women, and in particular celebrities (DeepTrace, 2019). However, and an increasing number of non-celebrity women are becoming victims. For example, a number of women in Cork, Ireland, found their Facebook photos had been stolen and used to create pornography (Edwards and Roche, 2016) and a Telegram AI-bot targeted more than 100,000 women, creating, and distributing fake pornographic images to almost 25,000 Telegram subscribers, including the women themselves, their family, and friends (Sensity AI, 2020).

(1) The creation of a false idenity of someone so that the person appears to have done specific things such as providing political opinions.

An increasing number of victims can be seen on burgeoning numbers of dedicated platforms for the distribution of deepfake pornography such as AdultDeepFakes.com and CelbJihad.com (Simonite, 2019). Platforms such as MrDeepFakes.com provide users with training guides, and forums for members to share tips and seek advice. There have been attempts by some dedicated pornography websites to stop the distribution of deepfake pornography, such as the Canadian-owned Pornhub (Hern, 2018), as it notes in its 2019 report (2019, p. 38) when "celebrities are in the news and on everyone's mind, they tend to drive a lot of Pornhub searches", resulting in more than 50 million searches before its ban came into effect.

The impact on women who are victim-survivors can be profound experiencing humiliation, shame and embarrassment with intimate partners, family, friends, work colleagues and in public, and sexual shame and sexual problems, body image issues, education and employment disruptions, concerns for personal safety, becoming paranoid and hyper vigilant, and trust issues to name just a few (Lichter, 2013). Some women have spoken out about their experiences. Karen Mort, a poet and broadcaster in Sheffield, UK, became a victim when someone stole non-intimate images of her from her private social media accounts, uploaded them and invited others to make deepfake pornography with them (Hao, 2021). She is reported as saying: "It really makes you feel powerless, like you're being put in your place," "Punished for being a woman with a public voice of any kind. That's the best way I can describe it. It's saying, 'Look: we can always do this to you'" (Hao, 2021, p. 1).

Some men's manipulation of a women's online image or voice to produce deepfake pornography increases women's sense, and limitlessness, of perpetrator(s) omnipresence, so that they experience continued surveillance in virtual worlds (Woodcock, 2017). Because these spaces are transnational,

they produce a sense of spacelessness for abuses and violations across landscapes through diffusion, with victim-survivors experiencing abuses and violations in differing geographical, representational, symbolic, physical, emotional ways (Harris, 2018).

The risk of becoming a victim means that many women feel online spaces are becoming increasingly unwelcome, exclusionary, silencing and isolating, because misogynistic beliefs and practices that are cloaked by anonymity and impunity. Citron (2016, in Ajder et al., 2019, p. 6) argues that:

"Deepfake technology is being weaponized against women by inserting their faces into porn. It is terrifying, embarrassing, demeaning, and silencing. Deepfake sex videos say to individuals that their bodies are not their own and can make it difficult to stay online, get or keep a job, and feel safe."

Although far less is known about individual men's motives for creating deepfake pornography, researchers (e.g., Checa and Bustillo, 2020; Thrift, 2008) point out that the abuse of modern technologies allows some men to explore sexual freedoms from unrestricted sexual urges typically governed by social norms and laws on gender-sexual relationships in the physical world. As such, some men can create new spaces for unlimited sensuality, enchantment, and experimentation of abusive acts to women of their choice (Obrador-Pons, 2007). Women who become victims are reduced to sexual objectifies and commodities. In this sense, women's bodies are not only a physical or virtual prosthetics, but can become something more through modern technologies, limited only by the perpetrator's imagination (Attwood, 2011; Hearn and Hall, 2022).

But despite the clear harms to women, there is still a relative absence of laws to prevent or prosecute perpetrators or regulate the development or use of new technologies specifically for abuse and violation (Banet-Weiser, 2019; Öhman, 2020). The relative absence of laws has led to some legal scholars,

such as Professor McGlynn QC, to warn of a potential future 'epidemic' in deepfake pornography (Selbie and Williams, 2021). In the following section we explore some of the socio-cultural-political-legal challenges to protect women from harm in physical and virtual spaces.

Women's Rights Are Human Rights

Although many countries signed up to the Universal Declaration of Human Rights (UDHR) and the subsequent treaties such as the International Covenant on Civil and Political Rights (ICCPR) (UN, 1966a) and the International Covenant on Economic, Social and Cultural Rights (ICESCR) (UN, 1966b), the protection of women from (non)physical, psychological, and emotional abuses in the physical world, these are not uniform across countries due to differences in socio-political-cultural norms and values about gender and gender relationships (Byrnes and Freeman, 2011). For example, Jaising (2018) highlights how 'dowry deaths'(1) in India are a consequence discriminative cultural practice and the unequal application of laws to Muslim, Hindus, and Sufis. Another challenge to the UDHR principles and legal dimensions of the subsequent treaties is that often women's rights and human rights more generally, are viewed as largely something concerning governments, and not for organizations, communities, and individual citizens, unless laws exist to make practices illegal. Many countries do however, equality laws or acts to protect specific groups, including women of all ethnicities, for example, in the UK Equality Act 2010 (UK Government, 2015), which can be applied to both physical and virtual worlds. And there are a growing number of countries such as in the Philippines, Israel, Canada, Germany, Japan, UK, New Zealand etc. who have implemented laws specifically to address the increasing array of ways that modern online technologies are used to abuse and violate women. However, as the Law Commission for England and Wales (2021, p. 1) points

(1) Married women murdered or driven to suicide becuase of disputes over the money, goods, or estate she brings to her marriage.

out, laws in the UK, and elsewhere, have not typically, "kept up with this behavior, resulting in significant gaps that have left victims unprotected." But, whilst there are clearly efforts by some countries to address the treats to women from new technologies, there are still a significant number of countries that do not have legislation in place for the prevention and prosecution for the abuse and violation of women in online virtual worlds (Mania, 2020).

The absence of universal laws and relative absence of specific laws in each country to protect women from abuse and violation in online spaces is further complicated where they occur across geopolitical boundaries. For example, before the dedicated 'revenge pornography' website MyEx.com was taken down by US legislators (Eslinger, 2018), it contained more than 10,000 images of women, and was reported to be owned by anonymous US individuals, operated in coordination with colleagues in the Philippines, hosted by Web Solutions B.V., Netherlands, with a global reach (Steinbaugh, 2014). The transnationalization of abuse and violation also means it can be difficult for victim-survivors to seek prosecutions and/or bring civil claims for damages against perpetrators. For example, it took American activist and YouTube star Chrissy Chambers six years to secure a conviction and receive compensation in the UK High Court after her UK partner had secretly filmed and uploaded videos of her to a free-to-watch pornographic website after they split because the images were taken and posted before it was illegal in the UK, further complicated due to the involved differnt legal jurisdictions which have different laws. (BBC, 2018).

Some legal solutions and their challenges

The argument should be that it is the lowest cost avoider principle that has to lead and direct the legislative efforts. The reason is the complexity of possible perpetrators that can be held responsible and those who have responsibilities in stopping such behavior.

Given the relative absence of international laws, and specific laws in some individual countries, we explore the possible legal solutions and their challenges that may respond to the increasing threat to women of new, advanced and emerging technologies such as AI, AR, VR, MR and if, or when, it becomes a reality SR.

The legal challenges that face women's rights protection in the case study of deepfake pornography are numerous. These include but are not confined to, positive law issues such as the relative absence of international laws, and specific laws in some individual countries. Thus, even if there is some regulation that already applies to deepfakes, the question often remains about its practical applicability. That is evident from other issues such as jurisdictional and enforcement obstacles to protecting women from such abuse. Imagine a perpetrator who makes and distributes deepfake images of female public figure in order to discredit her. For example, there was a doctored video of the then House Speaker Nancy Pelosi who appeared to be drunk on a fake video (O'Sullivan, 2019). That can be done from anywhere in the world, where, even if law exists that forbids such behavior, it cannot be enforced because of the lack of international enforcement agreements. Extraditing perpetrators and enforcing foreign judgments require such international treaties to which the country where the perpetrator is a signatory. To make things more complicated there has to be a political will in order to enforce such judgments. Today, if a person decides to engage in those activities in Russia, for example, it will be impossible to enforce a judgment against him or to extradite him or her.

The most comprehensive protection of women's rights comes from Europe, where the ECHR has been protecting human rights successfully albeit with some jurisdictional and enforcement challenges in the east part of the continent. The most interesting regulatory regime that will be examined is the EU's.

The EU Regulatory Regime as a High Standard Example

In the European Union, a comprehensive legal approach that regulates the use of AI, including for the purpose of protection against the use of deepfake pornographic images, is at a development stage at the moment. This proposal of the European Parliament and Council (2021) is the cornerstone of the EU regulatory framework that includes other legislation that can be used to protect women's rights against the misuse of AI.

Another existing regulation in the EU that that sets one of the best protections of privacy and security law in the world is The General Data Protection Regulation (GDPR). It provides support for the rights of EU citizens even beyond the Union's territory because it holds responsible organizations and individuals anywhere in the world if they target or collect data related to EU citizens. The regulation has been into effect since May 25, 2018. The provisions of GDPR have sanctions that can be substantial for amounts of millions of euros. This regulation is relevant to deepfake pornographic images because it protects personal date of an individual by which a woman can be identified, such as image or face. Deepfake pornography cannot usually be created without the use of such personal data. Personal date use may concern the provision of GDPR.

Copyright protection is another EU regulatory instrument that can be used for dealing with infringement of women's rights with the creation of deepfake images. Here we can talk about photography and cinematographic work that are protected. The issue is whether every image counts as "work" under the copyright law. Nevertheless, because of the efforts in EU legislation the area of law is harmonized across the EU, despite being a prerogative of the member states in general (European Parliament 2021)

The EU regulatory regime is such a good example of successful regulatory regime at protecting women's right because it works hand in hand with an

international convention and an international court. The European Convention on Human Rights (ECHR) is an international law instrument that is part of the greater Europe as opposed to just the European Union and it thus operates on much larger territory. It protects the use of personal data because its misuse may infringe upon the right to respect for private and family life contained in Article 8 of ECHR. The guardian of the convention the European Court of Human Rights is also being involved in protection of personal images that are not generally protected by copyright because they do not qualify as "works". In the case of Reklos and Davourlis v Greece on January 15, 2009, the European Court of Human Rights, used article 8 of the convention to render a ruling that protects the image of a baby taken without permission of a photographer. These possibilities for protection of women's rights exist on the European continent and as long as they can be enforced and overcome political hurdles they are extremely useful. These are possibilities for securing the rights of women who have been subject to abuse with deepfake pornographic images and videos. There are very few other places in the world where national, supranational and international level of law work as well as in Europe and more specifically in the European Union. Nevertheless, the main legislation on the issue is still at proposal stage.

The United States Regulatory Regime

In the US, there have also been some attempts to protect women against deepfake pornographic images. The efforts have been mostly on state as opposed to federal level despite that there have been legislative proposals from representatives of both parties—the republicans and the democrats. However, the obstacles in the US on federal level can be quite substantial. They can be even at constitutional level. The First Amendment can prevent a victim to sue a producer of the video who can claim freedom of speech protection of the image he or she has created (Gieseke, 2020). On legislative

level, section 230 of the Communications Decency Act ("CDA") can also stop a claim in its tracks when they decide to sue the platforms that distribute the deepfake image. Websites that host deepfake because the legislation was created at the dawn of the Internet Age, and it was mostly created to allow the internet to develop by limiting liability of platforms from the actions of third parties who upload content on them (Gieseke, 2020).

On state level, in July 2019, Virginia has expanded its law against harassment through the sharing of sexual images to cover deepfake images and videos. It criminalizes the dissemination of such content if it is intended to coerce, harass or intimidate a person. The law took effect on January 1, 2020. The sanction is classified as misdemeanor and not clearly distinguishable from the one for revenge porn, which is different because of the possible number of victims.

That is a step forward for victims of revenge porn, but legislating such issues can be difficult. Victims' groups in the UK say that revenge porn laws aren't working because victims are not guaranteed anonymity, leaving many afraid to speak out.

Another law in California (AB 602)[(1)] introduced a private right of action for individuals seen in pornographic deepfakes to simplify the individual complaint process. AB 602 provides a private cause of action against a person who either:

1. Creates and intentionally discloses sexually explicit material if that person knows or reasonably should have known the depicted individual did not consent; or
2. Intentionally discloses sexually explicit material that the person did not create if the person knows the depicted individual did not consent.[(2)]

(1) Cal. Civ. Code § 1708.85(b) (2020).
(2) Cal. Civ. Code § 1708.85(b) (2020).

The sanctions can go beyond economic, noneconomic, and emotional distress damages are possible. The statutory damages can be from $1,500 and are limited to $30,00. If there was malice the damages can go up to $150,000. Punitive damages, attorney's fees and costs; and injunctive relief are also probable.

A New York law passed in late 2020 also introduces the right of private action against pornographic deepfakes. The focus of that law, however, is unique. The reason is it establishes a new right of publicity to protect an artist's likeness - and hence possible deepfakes of that person -from unauthorized commercial exploitation for 40 years after his or her death. The pornographic deepfake issue is addressed at section CVR § 52-C of this New York Privacy Law. It came into force on May 29, 2021.

The law provides for injunctive relief, which means that a court may issue an emergency order to take the images down from the relevant websites. Punitive damages, compensatory damages and "reasonable court costs" and attorney's fees are also possible under Section 52-C-5.

As state above, Section 230 of the Communications Decency Act continues to be a serious obstacle to protecting women against deepfakes. That is confirmed in Section 52-C.10 of the New York Privacy Law, which specifies that the law cannot be construed as limiting or enlarging the protection granted to providers. That automatically diminishes the effectiveness of the law and limits its application.

The other major problem of suing the producer who may be difficult to identify or might have disappeared also remains. The jurisdictional issue also remains if the defendant is outside the United States, and U.S. law may not be able to reach him or her. What is more, websites may have shared the content and finding and taking down the content from all of them might be an extremely arduous process.

The United Kingdom Regulation

A report called "Shattering Lives and Myths: A Report on Image-Based Sexual Abuse", led by Professor Clare McGlynn from Durham University, served as a wakeup call for the legal community in the UK on among others the issue of deepfake pornography. That was followed by a communiqué of the Ministry of Justice that was published 26 June 2019 announcing the creation of a Law Commission that was to examine "whether current legislation is fit to tackle new and evolving types of abusive and offensive communications, including image-based abuse, amid concerns it has become easier to create and distribute sexual images of people online without their permission." The result was the Online Safety Bill[1] that at the time of writing is at second reading state at the House of Commons. To become an Act that is in force, the House of Lords has to hear the bill on 3 hearings and the purely ceremonial assent of the king is needed.

Section number 163 entitled "Sending photograph or film of genitals" seems to be relevant to deepfake pornography.

The following subsections seem to define the main terms: (3) "Photograph" includes the negative as well as the positive version. (4) "Film" means a moving image. (5) References to a photograph or film also include— (a) an image, whether made by computer graphics or in any other way, which appears to be a photograph or film.

Subsections that are the most relevant and the closest to AI created deepfake pornographic image or as it was called in the Bill "computer generated graphics." The sanction is contained in subsection (6) and states:

A person who commits an offence under this section is liable—

(a) on summary conviction, to imprisonment for a term not exceeding the general limit in a magistrates' court or a fine (or both).

(1) Available at: https://publications.parliament.uk/pa/bills/cbill/58-03/0209/220209.pdf

(b) on conviction on indictment, to imprisonment for a term not exceeding two years.

Section 69 (3) seems to impose a duty on providers to only "to make and keep a written record, in an easily understandable form."

In Chapter 2 Illegal content duties for all user-to-user services sections 8 Illegal content risk assessment duties and 9 Safety duties about illegal content

It does not appear as the Bill is clearly addressing the issue of deepfake pornography abuse of women. As a result, the courts in future cases will be called upon to clarify the law, provide its interpretation and set the boundaries of the application of this vague rule. That means that it will be years before women receive clear legal protection in such abuse in the UK. Even more disturbingly, it seems like providers will be mostly required to remove content that breaches their own rules, but it is not clear how far the liability will go in the specific case of deepfakes. In a situation where the producer cannot be found that seems that liability in the context of deepfake images will have limited effect.

Distinguishing Deepfakes from Similar Violations

Before we move to the possible regulatory solutions, it is important to distinguish between Deepfakes and similar violations sanctioned by law. The reason is those differences are substantial and are relevant in creating legal rules that stop such undesirable infringement upon individuals. In revenge porn the perpetrator is clear—he or she is the ex-partner of the victim. In contrast, the producer of a deepfake might not be easy to identify. Deepfakes can also be distinguished from privacy infringements because technically speaking deepfakes are produced with a photograph of a person who himself or herself posted online. That means there was no intrusion at any moment of the privacy of the victim who made the choice to make his or her picture

public (Gieseke, 2020). Also, deepfakes are borderline case that is grounded both in reality and the fake because they use a real image and create an unreal image. Thus, they cannot be treated completely as a copyright or privacy because contrary to them they are not entirely real. They are subject to a creation process that creates a fake.

Copyright and data protection

The regulation of copyright is also different from deepfake pornography because the person affected might have different rights from that of the perpetrator. The simplest case is that the victim has to have a registered right on the photo. If she does own a copyright on the image she cannot get protection. In deepfake, AR, VR, and MR where images are used copyright of images is likely to be a key consideration. Indeed, even in textual, semantic generated images, such as Stable Diffusion(1) copyright considerations feature, and was the catalyst for Stable Diffusion 2, so that artists' work could be protected from copying (Romero 2022). There is also the complication of copyright and data protection. For example, the World Intellectual Property Organization (2020), published a Conversation on intellectual property (IP) and artificial intelligence (AI) highlighting how questions of consent, ownership, the right of use and distribution, hinders the prosecution of deepfake pornography perpetrators in most countries (WIPO, 2020, p. 9). The WIPO argues that because of issues related to human rights, protection from harm, privacy, data protection, etc. by giving copyright to deepfake images whether pornographic or not, may in some cases protect the perpetrators, where the perpetrator has produced the images, despite using someone else's images to do so. Indeed, there is the added problem of determining in court whose images are being amalgamated, who owns those images, what is being represented, what the representations are about, and what was the intend in amalgamating those

(1) Stable Diffusion is a deep learning, text-to-image algorithmn used to generate detailed images conditioned on text descriptions.

images (Burkell and Gosse, 2019).Therefore, the Internet Justice Society (Çolak, 2021) suggests prosecutions could be based on infringements of the legislations and regulations such as EU General Data Protection Regulation (GDPR) under the maintenance of accurate data, which deepfake pornography clearly contravenes.

Tort law

Where laws exist in specific countries, perpetrators can be tried by criminal laws. However, only prosecuting perpetrators do not address the damage done to victim-survivors as we noted above. Thus, Tort/Civil laws could be drawn upon, where they exist, so that the victim-survivor can sue for damages to, for example, reputation or the cost of work and educational disruptions. For example, Tort/Civil Laws in the UK has historical writs on trespass Vi et Armis which allow claims where personal injury had been suffered as a result of the defendant's direct and forceful misconduct (McNellis, 2019). This is likely to have featured as part of Chrissy Chambers' protracted legal case against her ex-spouse with the eventual award of an undisclosed sum of compensation by the UK High Court (BBC, 2018).

Tort and copyright law could provide a cause of action for some victims, their inability to address the vast majority of situations nullifies their viability. Subsection B.3 analyzes the inadequacy of state revenge pornography statutes and federal legislation. Although those statutes seem to provide the most analogous protection for deepfake victims, they are also geared toward protecting against the revelation of real images (Gieseke, 2020).

In the UK, it is very difficult to create a new tort. That means the creation of a tort that protects victims of deepfake pornography seems unlikely. The adoption of the UK Human Rights Act 1998, has not given an impetus to courts to create new torts. Lord Hoffmann in Wainwright v Home Office(1)

(1) [2003] UKHL 53; [2004] 2 AC 406.

maintained that there is no need to "distort" the principles of the common law and quoted Sir Robert Megarry V-C in Malone v Metropolitan Police Commissioner[1]: "[I]t is no function of the courts to legislate in a new field. The extension of the existing laws and principles is one thing, the creation of an altogether new right is another."[2]

Regulating Deepfake Pornography

Because Europe sets to set the golden standard for protection of human rights, we use similar structure as the one in a report prepared for EU Parliament (2021) where the policy recommendations are comprehensive on how to reduce the abuse AI created deepfake pornographic images. They found the following regulatory options to deal with: 1. Technology, 2. Creation, 3. Circulation, 4. Target, 5. Audience. That means regulating the technology creator, the creator of the deepfake, the platform that circulates it, the target is to protect the victim through easier mechanisms to sue for example, and the audience is the final users or the people who watch it. In order to choose which one of those methods has to be used the idea of the lowest cost avoider has to be used.

Lowest cost avoider

The main principle that has to be used in regulating deepfakes is the one of the lowest cost avoider. The reason is the deepfakes cause damage to the victim because of undesirable behavior on the part of more than one person. Thus, since deepfake technologies are created, produced, distributed, used and abuse different people, we begin here, within the law and economics concept of the 'lowest cost avoider' (Gilles, 1992). The concept centers on who can prevent the abuse or violation of women with new technologies for the least

(1) Malone v Metropolitan Police Commissioner [1979] Ch 344 at 372.
(2) Malone v Metropolitan Police Commissioner [1979] Ch 344 at 372.

cost. Despite the jurisdictional challenges, the lowest costs are likely to be borne by either designer and developers of new technologies, or where no single producer has a monopoly on the technology, then the platforms hosting and where the dissemination of abuses and violations occur. This is because it is legally much easier to identify the platform for the abuse and violation than it is to track the perpetrator who is likely to have posted anonymously from anywhere in the world on any device. Indeed, even pinpointing the device used for the abuse or violation, is not always enough evidence to secure a conviction (Brown, 2015).

Designers and developers

Some scholars such as Raso et al. (2018) argue that the onus for the (mis) use of technologies should be placed on designers and developers. They argue that because people design and develop to achieve specific outcomes they bring their own existing biases and prejudices to the design and development process. Recent survey research by the AI Now Institute, New York University, US (Whittaker et al., 2018) found those in the field of AI were predominantly white men highlighting the risk of replicating or perpetuating historical gender and ethnicity stereotypes, biases and power imbalances, for example, when programming image classifications and the recognition of derogative language. Therefore, Raso et al., (2018) argue that there should be more transparency and accountability in designing and developing new technologies about the rationales behind them, the decision-making processes involved, and ethical and in-built safeguard considerations, otherwise it is difficult to access their potential for their (un)healthy uses. Wachter, Mittelstadt, and Floridi (2017) suggest that if reporting was a legal requirement then legal mechanisms for accountability for harms could be invoked under a 'right to explanation' under the EU General Data Protection Regulation (GDPR) (European Council, 2018). However, as Edwards and Veale (2017) point out, the GDPR may not

be able to remedy harms to women because it does not make clear when and in what cases an explanation would be required or what information in any explanation is meaningful, or whether all reporting information will be divulged because of concerns about intellectual property and trade secrets. Bartlett (2019) also notes that designers and developers are often individual people and small enterprises and so if they faced legal action for the abuse of their designs, it may stifle innovation because the risks may outweigh the benefits. Indeed, the risk of legal action may also impinge on the willingness of investors to fund new technologies in their infancy.

When technologies are designed and developed to target women specifically, this causes harm such as the DeepNude application (European Parliament's, 2021). Tackling deepfakes in European policy could be used by countries in the EU, as it specifically targets the malicious use of deepfake technologies for such purposes. DeepNude was specifically designed to allow users to upload images of women so that they could 'undress' them, showing the viewer realistic images of what they would look like naked (Mahdawi, 2019). Such examples would also fall within the remit of the European Union Agency for Fundamental Human Rights' (2020) Artificial intelligence and big data (FRA, 2018), which covers the malevolent design of algorithms.

Internet service providers and social media platforms

There have been developments in algorithmic moderation systems such as automated hash-matching and predictive machine learning tools to address abusive user-generated content on Facebook, YouTube, Reddit and Twitter (Gorwa, Binns and Katzenbach, 2020). However, there is yet no legal requirement in many countries for them to be proactive in stopping these abuses, only their removal within a reasonable period of time (Walsh and O' Connor, 2019). A notable exceptions is the UK's Online Safety Bill, which means social media organizations are legally required to remove illegal content

and material breaching their own terms of service but will not define specific types of legal content that the organizations must address (UK Government, 2022). This allows for a broad interpretation of what constitutes legal content under the Bill, especially when it conflicts with notions of the freedom of speech (Loomis, 2022). There also remains the question of the time to remove illegal or abuse content. Indeed, abusive materials can distributed widely in a relatively short space of time, as a victim-survivor of colloquially called 'revenge porn' found when ex-partner posted explicit images of her online and within hours they were on 200 websites (BBC, 2014). However, governments are likely to continue to pressure online platforms and social media companies to develop technical solutions, but developments are likely to be unable to keep pace with new technological developments and forms of abuses and violations of women.

Who is the Lowest Cost avoider in deepfake pornographic images?

The creator of the deepfake image

If the creator of the deepfake pornographic image can be found and there are no jurisdictional issues he or she can also be the lowest cost avoider and should be held responsible. After all, it is the direct actions of such a person that led to the damage to the victim.

In any case, as a general rule, the law should affect the supply side of the market. For deepfakes the entity that should be held responsible should be the creator of the deepfake image when he or she is identifiable. The distributor of the technology is the most logical choice if the creator cannot be identified. These are usually platforms with millions if not billions of users with substantial financial ability to take preventive measures such monitoring their own content even in user-to-user distribution. Large platforms are perfectly capable to invest in the ability to distinguish deepfakes from other

videos. Sanctions directed at the supply side of new technology means that these companies will incur extra cost in having specifically trained staff (or AI technology) able to identify deepfakes. That will increase the cost of production and distribution of the technology. That cost has to be borne by the large distributors and not shifted to the final users of the technology.

Producers also bear responsibility because they can at low cost make technological innovations that allow the creator of the deepfake to be tracked and platforms to monitor the real content. However, the balance should be drawn with innovation, which should not be stifled.

Possible Defense: Consent

The question of consent also plays a fundamental role in deepfake pornography and other modern technologies in (dis)similar ways to the abuses and violations of women in the physical world and are influenced by cultural norms, motives, and the available legislation to prosecute perpetrators. For example, consent may have been given to take a sexualized image (e.g., taken by the person or for someone else to do so), and in some cases also to the distribute (e.g., on specific social media platforms such as Tik Tok), and use (e.g., for challenges such as #sillhoettechallenge,[1] #icecubechallenge[2]), but not to use, manipulate, or distribute elsewhere (e.g., by [un]known viewers), or to consent to receive by (un)known others. Questions of consent and where it was or was not given can have implications for perpetrator accountability or for the victim-survivor (Hall, Hearn and Lewis, 2022).

Consent can also have serious implications in prosecutions, the development of legislation, monitoring of posts on social media, and so on. Laws often also require proof that the perpetrator intended to cause distress,

(1) #sillhoettechallenge is a TikTok challenge that involves images of the woman in everyday life before showing just her frame in a provocative and sexy pose typically against a red-lit background, often in a doorway.

(2) #icecubechallenge is a TikTok challenge that involves women being filmed or filming themselves from the waste up inserting an ice cube into their vagina.

partly so that excessive criminalization is prevented. However, Huber's (2018) interviews with activists point out, non-consensual image taking, making, and distribution are always likely to cause distress. Even when victim-survivors do come forward, they are often not protected by anonymity, and so risk public shame, embarrassment, and further abuse because of cultural notions of accountability. This can be especially so where consent to take the image was presumed to have been given, for example, via sexting or TikTok videos (Marcum, Zaitzow and Higgins, 2021; Starr and Lavis, 2018). The European Parliament's (2021) proposed deepfake policy, which would obligate creators of deepfake images to label those images so that it is clear who manipulated, which could be used in copyright legal cases. However, we wonder how many of those people creating deepfake pornographic images are likely to comply with this and how easy it would be to enforce this, especially since around 96% of the internet is unmonitored or regulated in the 'dark web' (Deyan, 2021).

Even when consent to take an image was initially given, some commentators (Tyler, 2016) argue that consent is questionable even in the production of sexual materials such as home porn movies and sexting where initial consent is presumed. This is for three reasons. Firstly, women's continued economic, political, social, and sexual inequality contributes to a form of cultural coercion into various forms of porn production. Secondly, sexual violence and abuse against women is common in all forms of porn. And, finally, the porn industry rests on the worldwide sexual objectification of women. Thus, at a more general level of gender and economic class structures, all porn can be potentially understood as coercive or non-consensual because its existence contributes to gendered inequality, and men, as a class, benefit, collectively, at the expense of women.

Conclusion

Modern technologies are here to stay. However, it is clear that they are becoming increasingly misused to harm women (European Institute for Gender Equality, 2022). Because of the limits of a journal paper, we opted to focus on the phenomenon of deepfake pornography among a myriad of other threats to women's rights that result from the use of AI. We argued that legislative efforts should focus on sanctioning the lowest cost avoider among all possible entities and individuals who can be held responsible for this socially undesirable behavior. We showed the enormous costs that AI technology may impose on women when it is left unchecked. These costs do not allow women to function as free productive members of society. The legislative challenges that we identified occur across multiple geopolitical and legal jurisdictions because violations happen in online spaces that know no national boundaries, thus it makes them hard to regulate. To better understand how to prevent and peruse perpetrators of infringements against women's rights in the physical world, we examined the legal foundations on preventing significant infringements of women's rights as enshrined in the UDHR and subsequent treaties (UN, 1966a; 1966b). Then, we focused on the newest legislative efforts in the US, the UK and the EU. Though commendable, these are still piecemeal regulatory moves that are likely to be slow and leave many women unprotected across the world. Moreover, these new regulations are not free of specific weaknesses some of which we have identified. As a solution, we highlighted the need to have a more widespread comprehensive regulatory framework. Thus, as mentioned above, we argued for a common principle such as holding the lowest cost avoider responsible. That is a simple and workable approach that can reduce the abuse of women's rights resulting from the misuse of deepfake pornography AI.

References

- Ajder, H., Patrini, G., Cavalli, F., & Cullen, L. (2019). The state-of-the-art deefakes: Landscape, threats, and impact. Deeptrace. September. Retrieved from: file:///F:/Publications/Academic%20Publications/Books/Digital%20Sexual%20Violences/Literature/Deeptrace%20deepfake_report.pdf
- Attwood, F. (2011). Through the looking glass? Sexual agency and subjectification online. In R. Gill & C. Scharff (eds). New femininities (pp. 203-214). Palgrave Macmillan, London.
- Azuma, R. T. (1997). A survey of augmented reality. Presence: teleoperators & virtual environments, 6(4), 355-385. https://doi.org/10.1162/pres.1997.6.4.355
- Bailey, J., & Burkell, J. (2021). Tech-facilitated violation: thinking structurally and intersectionally. Journal of gender-based violation, 5(3), 531-542. https://doi.org/10.1332/239868021X16286662118554
- Bailenson, J. (2018). Experience on demand: What virtual reality is, how it works, and what it can do. New York: WW Norton & Company.
- Banet-Weiser, S. (2021). Misogyny and the politics of misinformation. London: Routledge.
- BBC (2014). Revenge porn victim: I trusted him, now I'm on 200 sites. April 3. Retrieved from: https://www.bbc.com/news/av/newsbeat-26852254
- BBC (2018). YouTube singer Chrissy Chambers wins revenge porn case. January 17. Retrieved from: https://www.bbc.com/news/technology-42720869
- Byrnes, A., & Freeman, M. (2011). The Impact of the CEDAW Convention: Paths to Equality. A Study for the World Bank. Background paper for

the WDR 2012. Retrieved from: https://openknowledge.worldbank.org/bitstream/handle/10986/9219/WDR2012-0014.pdf

- Brown, C. S. (2015). Investigating and prosecuting cybercrime: Forensic dependencies and barriers to justice. International Journal of Cyber Criminology, 9(1), 55-119. 10.5281/zenodo.22387
- Burkell, J., & Gosse, C. (2019). Nothing new here: Emphasizing the social and cultural context of deepfakes. First Monday. Retrieved from: https://journals.uic.edu/ojs/index.php/fm/article/download/10287/8297
- Carmigniani, J., Furht, B., Anisetti, M., Ceravolo, P., Damiani, E., & Ivkovic, M. (2011). Augmented reality technologies, systems, and applications. Multimedia Tools and Applications, 51(1), 341–377. https://doi.org/10.1007/s11042-10-660-6
- Castronova, E. (2008). Synthetic worlds. USA: University of Chicago press.
- Checa, D., & Bustillo, A. (2020). Advantages and limits of virtual reality in learning processes: Briviesca in the fifteenth century. Virtual Reality, 24(1), 151-161. https://doi.org/10.1007/s10055-019-00389-7
- Citron, D. K., & Chesney, R. (2018). Deep fakes: A looming crisis for national security, democracy and privacy? Lawfare. February 21. Retrieved from: https://perma.cc/L6B5-DGNR
- Çolak, B. (2021). Legal Issues of Deepfakes. Internet Justice Society, January 19. Retrieved from: https://www.internetjustsociety.org/legal-issues-of-deepfakes
- DeepTrace (2019). The state of deepfakes: Landscape, threats, and impact. Retrieved from: https://regmedia.co.uk/2019/10/08/deepfake_report.pdf

- Deyan, G. (2021). How much of the Internet is the Dark Web in 2021? Tech Jury. September 21. Retrieved from: https://techjury.net/blog/how-much-of-the-internet-is-the-dark-web/
- Edwards, E., & Roche, B. (2016). Use of women's Facebook pictures on porn site investigated. Irish Times. January 14. Retrieved from: https://www.irishtimes.com/news/crime-and-law/use-of-women-s-facebook-pictures-on-porn-site-investigated-1.2497092
- Edwards, L , & Veale, M (2017). Slave to the algorithm? Why a "right to an explanation" is probably not the remedy you are looking For. Duke Law and Tech Review, 16 , 18–84 .
- Eslinger, B. (2018). 'Revenge Porn' Site MyEx.Com Shut Down By Nevada Judge. Law 360. June 25. Retrieved from: https://www.law360.com/articles/1056556
- European Council (2018). The general data protection regulation. May 25. Retrieved from: https://www.consilium.europa.eu/en/policies/data-protection/data-protection-regulation/#:~:text=The%20EU%20general%20data%20protection%20regulation%20(GDPR)%20is%20the%20strongest,application%20on%2025%20May%202018.
- European Institute for Gender Equality (2022). Combating Cyber Violence against Women and Girls. November 25. Retrieved from: https://eige.europa.eu/publications/combating-cyber-violence-against-women-and-girls
- EU Parliament (2021). Tackling deepfakes in European policy. July. Retrieved from: https://www.europarl.europa.eu/RegData/ etudes /STUD/2021/690039/EPRS_STU(2021)690039_EN.pdf
- European Parliament and Council (2021). Proposal for a regulation of the European Parliament and of the Council: Laying down harmonised rules

on the artificial intelligence (Artificial Intelligence Act) and amending central Union legislative acts. Retrieved from: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206

- European Union Agency for Fundamental Human Rights (2020). FRA - Promoting and protecting your fundamental rights across the EU: Artificial intelligence and big data. Retrieved from: https://fra.europa.eu/en/themes/artificial-intelligence-and-big-data
- Farshid, M., Paschen, J., Eriksson, T., & Kietzmann, J. (2018). Go boldly!: Explore augmented reality (AR), virtual reality (VR), and mixed reality (MR) for business. Business Horizons, 61(5), 657-663.
- Franks, M. A. (2016). Drafting an effective "revenge porn" law: A guide for legislators. Cyber Civil Rights Initiative. Retrieved from: www.cybercivilrights.org/guide-to-legislation/
- Franks, M. (2017). The desert of the unreal: inequality in virtual and augmented
- reality. U.C. Davis Law Review, 51(2), 499-538. Retrieved from: https:/ /repository .law.miami.edu/cgi/viewcontent.cgi?article = 1538& context=fac _articles
- Gieseke, A. P. (2020). "The New Weapon of Choice": Law's Current Inability to Properly Address Deepfake Pornography. Vand. L. Rev., 73, 1479. Retrieved from: https://heinonline.org/HOL/LandingPage?handle=hein.journals/vanlr73&div=39&id=&page=
- Gilles, S. G. (1992). Negligence, strict liability, and the cheapest cost-avoider. Va. L. Rev., 78, 1291. Retrieved from: https://heinonline.org/HOL/LandingPage?handle=hein.journals/valr78&div=58&id=&page=
- Gorwa, R., Binns, R., & Katzenbach, C. (2020). Algorithmic content moderation: Technical and political challenges in the automation of platform governance. Big Data & Society, 7(1), 2053951719897945

- Hall, M., Hearn, J. & Lewis, R. (2022). Digital Gender-Sexual Violations: Violation, Technologies, Motivations. London: Routledge.
- Hao, K. (2021). Deepfake porn is ruining women's lives. Now the law may finally ban it. Technology Review. February 12. Retrieved from: https://www.technologyreview.com/2021/02/12/1018222/deepfake-revenge-porn-coming-ban/
- Hauer, J.U. (2022). Virtual Human Services Delivery: Lessons for Equity, Leadership, and the Future. In J.U. Hauer. Multidisciplinary Approach to Diversity and Inclusion in the COVID-19-Era Workplace (pp. 247-261). Pennsylvania, US: IGI Global.
- Hearn, J. & Hall, M. (2022). From physical violence to online violation. Forms, structures and effects: A comparison of the cases of 'domestic violence' and 'revenge pornography'. Aggression and Violent Behavior, 67 (November/December). https://doi.org/10.1016/j.avb.2022.101779
- Henry, N., & Powell, A. (2014). The dark side of the virtual world. In N. Henry & A. Powell (eds). Preventing Sexual Violence (pp. 84-104). London: Palgrave Macmillan.
- Hern, A. (2018). 'Deepfake' face-swap porn videos banned by Pornhub and Twitter. The Guardian, February 7. Retrieved from: https://www.theguardian.com/technology/2018/feb/07/twitter-pornhub-ban-deepfake-ai-face-swap-porn-videos-celebrities-gfycat-reddit
- Hern, A. (2022). Online safety bill will criminalise 'downblousing' and 'deepfake' porn. The Guardian, November 24. Retrieved from: https://tinyurl.com/yckn9pn5
- Hilliker, S.M. (2022). Second Language Teaching and Learning through Virtual Exchange. The Hague, Belgium: De Gruyter Mouton

- Holz, T., Campbell, A. G., O'Hare, G. M. P., Stafford, J. W., Martin, A., & Dragone, M. (2011). MiRA – Mixed reality agents. International Journal of Human–Computer Studies, 69(4), 251–268. https://doi.org/10.1016/j.ijhcs.2010.10.1
- Jaising (2018). Violence against women: The Indian perspective. In J.S. Peters & A. Wolper (eds) Women's Rights Human Rights (pp. 51-56). London: Routledge.
- Lichter, S. (2013). Unwanted exposure: Civil and criminal liability for revenge porn hosts and posters. JOLT Digest: Harvard Journal of Law and Technology. May 28. Retrieved from: http://jolt.law.harvard.edu/digest/privacy/unwanted-exposure-civil-and-criminal-liability-for-revenge-porn-hosts-and-posters.
- Loomis, A. (2022). Deepfakes and American Law. Davis Political Review. April 20. Retrieved from: https://www.davispoliticalreview.com/article/deepfakes-and-american-law#:~:text=After%20all%2C%20posting%20deepfakes%20or,post%20pornographic%20or%20informational%20deepfakes.
- Mahdawi, A. (2019). An app using AI to 'undress' women offers a terrifying glimpse into the future. The Guardian. June 29. Retrieved from: https://tinyurl.com/4hx5btfe
- Mania, K. (2020). The Legal Implications and Remedies Concerning Revenge
- Porn and Fake Porn: A Common Law Perspective. Sexuality & Culture, 24(6), 2079-2097. https://doi.org/10.1007/s12119-020-09738-0
- Marcum, C. D., Zaitzow, B. H. & Higgins, G. E. (2021). The role of sexting and related behaviors to victimization via nonconsensual pornography: an exploratory analysis of university students. Journal of Aggression,

Conflict and Peace Research, September 11. Retrieved from: https://www.emerald.com/insight/content/doi/10.1108/JACPR-02-2021-0578/full/html?casa_token=eEsIvUduhSYAAAAA:PNj7bwhrKIiCVaY-TF41oIx_FhHGn65nwzsPztb3jX3erFwtWK0Zv5EiDrBa0qwDGLbt8FID2-aywsc3Lwr8M4zwA_YbaoK2rGMVv8P2rKVIqHY_5Ps

- McNellis, L. (2019). Vi et Armis: Londoners and Violent Trespass Before the Common Pleas in the Fifteenth Century. USA: West Virginia University.
- Obrador-Pons, P. (2007). A haptic geography of the beach: naked bodies, vision and touch. Social & Cultural Geography, 8(1), 123-141. https://doi.org/10.1080/14649360701251866
- Öhman, C. (2020). Introducing the pervert's dilemma: a contribution to the critique
- of Deepfake Pornography. Ethics and Information Technology, 22, 133–140.
- Oppenheim, M. (2022). Woman reveals 'nightmare' of being 'gang raped' in virtual reality. Independent, February 3. Retrieved from: https://www.independent.co.uk/news/uk/home-news/metaverse-gang-rape-virtual-world-b2005959.html
- O'Sullivan, D. (2019). Doctored videos shared to make Pelosi sound drunk viewed millions of times on social media. CNN, May 24. Retrieved from: https://edition.cnn.com/2019/05/23/politics/doctored-video-pelosi/index.html
- Özler, Ş. İ. (2018). The Universal Declaration of Human Rights at Seventy: Progress and Challenges. Ethics & International Affairs, 32(4), 395-406. https://doi.org/10.1017/S0892679418000588
- Pester, A., Madritsch, C., Klinger, T., de Guereña, X.L. (2020). Deep Learning Frameworks for Convolutional Neural Networks—A Benchmark

Test. In: Auer, M., Ram B., K. (eds) Cyber-physical Systems and Digital Twins. REV2019 2019. Lecture Notes in Networks and Systems, vol 80. Springer, Cham. https://doi.org/10.1007/978-3-030-23162-0_74

- Porn Dude (2022). Deepfake porn sites – deepnudes & fake celebrity nudes. Retrieved from: https://theporndude.com/fake-celebrity-nudes
- Pornhub (2019). The 2019 Year in Review. December 11. Retrieved from: https://www.pornhub.com/insights/2019-year-in-review
- Ramesh, U.V., Harini, A., Gowri, C.S.D., Durga, K.V., Druvitha, P., & Kumar, K.S. (2022). Metaverse: Future of the Internet. International Journal of Research Publication and Reviews, 3(2), 93-97.
- Raso, F. A., Hilligoss, H., Krishnamurthy, V., Bavitz, C., & Kim, L. (2018). Artificial intelligence & human rights: Opportunities & risks. Berkman Klein Center Research Publication, (2018-6). Retrieved from: https://dash.harvard.edu/handle/1/38021439
- Romero A. (2022). Stable Diffusion 2 Is the First Artist-Friendly AI Art Model. Towards Data Science. November 28. Retrieved from: https://towardsdatascience.com/stable-diffusion-2-is-not-what-users-expected-or-wanted-abfd39524dff
- Selbie, T. & Williams, C. (2021). Deepfake pornography could become an 'epidemic', expert warns. British Broadcasting Company. May 27. Retrieved from: https://www.bbc.com/news/uk-scotland-57254636
- Sensity AI (2021). The state of deepfakes 2020: Updates on statistics and trends. Retrieved from: https://sensity.ai/reports/
- Simonite, T. (2019). The web is drowning in Deepfakes and almost all of them are porn. Wired, October 13. Retrieved from: https://www.wired.co.uk/article/deepfakes-porn

- Sparkes, M. (2021). What is a metaverse. New Scientist, 251(3348), 18.
- Starr, T. S., & Lavis, T. (2018). Perceptions of revenge pornography and victim blame. International Journal of Cyber Criminology, 12(2), 427-438. Doi:10.5281/zenodo.3366179
- Statistica (2021). Augmented reality (AR) and virtual reality (VR) market size worldwide from 2016 to 2024. November 23. Retrieved from: https://www.statista.com/statistics/591181/global-augmented-virtual-reality-market-size/
- Steinbaugh, A. (2014). Revenge porn site myex.com sued for copyright infringement. March 7. Retrieved from: http://adamsteinbaugh.com/2014/03/07/revenge-porn-site-myex-com-sued-for-copyright-infringement/
- Thrift, N. (2008). Non-representational theory: Space, politics, affect. London: Routledge.
- Topping, A. (2016). Facebook revenge pornography trial 'could open floodgates'. The Guardian. October 9. Retrieved from: ww.theguardian.com/technology/2016/oct/09/facebook-revenge-pornography-case-could-open-floodgates.
- Tyler, M. (2016). All porn is revenge porn. Feminist Current, February 24. Retrieved from: http://www.feministcurrent.com/2016/02/24/all-porn-is-revenge-porn/
- UK Government (2015). UK Equality Act 2010. Retrieved from: https://www.gov.uk/guidance/equality-act-2010-guidance#:~:text=The%20Equality%20Act%202010%20legally,strengthening%20protection%20in%20some%20situations.
- UK Government (2022). New protections for children and free speech added to internet laws. November 28. Retrieved from: https://www.gov.

uk/government/news/new-protections-for-children-and-free-speech-added-to-internet-laws

- United Nations (1966a). International Covenant on Civil and Political Rights. General Assembly resolution 2200A (XXI), December 16. Retrieved from: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights
- United Nations (1966b). International Covenant on Economic, Social and Cultural Rights. General Assembly resolution 2200A (XXI), December 16. Retrieved from: https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-economic-social-and-cultural-rights
- UN-Habitat (2021). Assessing the Digital Divide: Understanding internet connectivity and digital literacy in cities and communities. November. Retrieved from: https://unhabitat.org/sites/default/files/2021/11/assessing_the_digital_divide.pdf
- Wachter, S, Mittelstadt, B , & Floridi, L (2017). Transparent, explainable, and accountable AI for robotics". Science Robotics, 2 (6), eaan6080 .
- Walsh, J. P., & O'Connor, C. (2019). Social media and policing: A review of recent research. Sociology compass, 13(1), e12648. https://doi.org/10.1111/soc4.12648
- Westerlund, M. (2019). The emergence of deepfake technology: A review. Technology Innovation Management Review, 9(11), 39–52.
- Whittaker,M., Crawford, K., Dobbe, R., Fried, G., Kaziunas, E., Mathur, V., Myers West, S., Richardson, R., Schultz, J. & Schwartz, O. (2018). AI Now Report 2018. AI Now Institute, New York University, US. Retrieved from: https://kennisopenbaarbestuur.nl/media/257225/ai_now_2018_report.pdf

- Woodcock, J. (2017). Working the Phones: Control and Resistance in Call Centres. London:
- Pluto Press.
- World Intellectual Property Organization. (2020). WIPO Conversation on intellectual property (IP) and artificial intelligence (AI): Revised issues paper on intellectual property policy and artificial intelligence. May 21. Retrieved from:
- https://www.wipo.int/edocs/mdocs/mdocs/en/wipo_ip_ai_2_ge_20/wipo_ip_ai_2_ge_20_1_rev.pf