Criminal Law in the Metaverse:

Addressing Sexual Harassment and Abuse in Virtual Realities

POLICY REPORT

University of Bristol - School for Policy Studies

DIGITAL TECHNOLOGIES, HARM, AND CRIMINAL JUSTICE

2064849

The rapid advancement of technology has paved the way for a new frontier of human interaction that blurs the lines between the physical and digital worlds. Immersion in a virtual universe where individuals can explore, socialise, and engage in a variety of activities seemed unimaginable 25 years ago. Today, this virtual landscape offers a multitude of opportunities, from gaming and education to professional collaboration and creative expression. This universe is called the metaverse, which means ‘’beyond the universe," and first appears in the novel Snow Crash, in 1992, which envisions a virtual reality-based successor to the internet (Haber, 2023).

It ranges from activities such as recreational and virtual reality games, education, and community building, which were particularly helpful during the Covid-19 pandemic (Onggirawan et al., 2023), to professional and commercial interactions such as NFTs or cryptocurrencies. It has been functional for practising skills and scenarios, such as medical procedures in surgery or practices in aviation (Syed Abdul et al., 2022). However, the metaverse not only replicates the physical, economic, or legal elements of the real world but also allows users to interact with others in new and realistic ways. As their popularity grew, virtual worlds such as online role-playing games began to offer more complex environments and realistic 3D graphics with themes such as fantasy or science fiction, including notable examples such as World of Warcraft, Roblox, Minecraft, or Fortnite. However, at the beginning of the 21st century, the metaverse allowed a more vivid and immersive gaming experience that goes beyond a game by creating a virtual world known as Second Life (other well-known examples include Habbo or The Sims). There, users can buy property to build a house, start a business, get married, or engage in sexual activities (Haber, 2023).

While the metaverse has brought countless opportunities and positive experiences, it has also led to new challenges and risks. Immersive virtual realities have come under increasing scrutiny in criminology because the user experience in the metaverse seems real. Cases of sexual assault, harassment, and privacy violations have occurred in the metaverse, raising important questions about the legal, ethical, and societal implications of these behaviours, although sometimes nothing translates into the real world (Cantley and Dietrich, 2022: 11). To apply certain law enforcement measures, it is necessary to understand the dynamics of virtual reality as real reality. This is challenging because what happens in the metaverse can be just as significant as what happens in real life (Chalmers, 2022). One of the most fundamental questions that

policymakers and law enforcement must ask is what constitutes misconduct in the metaverse and how it should be treated legally. Some crimes, such as theft, may be easier to prevent in the metaverse because ownership is detectable using advanced blockchain technology (Huynh-The et al., 2023). However, the borderless nature of this second life presents a potential disruption to criminal law, particularly for crimes of sexual abuse and harassment (Henry and Powell, 2016). This potentially disorienting technology could fundamentally change criminal law and its enforcement, starting with what should be considered a crime in the metaverse and how it should be classified. For this reason, it is important to analyse criminal behaviour in the metaverse and how harms are viewed from the current criminal law perspective (Haber, 2023:15).

This policy report will focus primarily on sexual abuse and harassment as major crimes in the metaverse. It first addresses the fundamental question of what should be considered a crime in the metaverse, focusing on establishing a theoretical framework for criminal behaviour in this virtual world. The report looks at key factors such as anonymity, accountability, surveillance, and deterrence, and analyses how these elements affect the definition and identification of criminal behaviour. In addition, the report examines how countries such as France and Norway have addressed harm in the metaverse with their existing criminal laws. In addition, the report examines the Digital Services Act as a contemporary legislative response to metaverse crimes and highlights the complexities and problems associated with this policy. It critically evaluates both the issues that have been addressed and those that have not been adequately resolved and offers insights into the strengths and weaknesses of the proposed approach.

What should be regarded as criminal behaviour in the Metaverse?

Experts have already hypothesised that the brain is tricked into believing virtual crimes are real and that they are happening, and that now the body has also learned to respond to virtual stimuli (Cantley and Dietrich, 2022:12). This immersive and fully interactive online environment is emerging, and it is no surprise that stranger harassment, also referred to in the criminal justice system as "technology-enabled abuse," has extended to these spaces as well (Wiederhold, 2022). Sexual harassment, stalking, or abuse is attributed to the anonymity that the Internet provides, as people (under their avatars) feel emboldened to act inappropriately when they believe they will not face consequences for their actions. A well-known case from 2021 comes from one of the

most prominent co-founders and VP of Metaverse research, Nina Patel, who shared her experience of sexual harassment at Metaverse venues. She recounted how her avatar was sexually harassed after several men surrounded her and touched and groped her body. And although Patel experienced that her physiological and psychological response was as it was (Zima, 2022), the case was not reported to the police and no complaint was filed (Singh, 2022). In such instances, the victims find themselves unable to pursue justice against the perpetrators, despite enduring an authentic assault within the virtual realm. The challenge lies in evaluating the extent of harm inflicted upon victims in cases of virtual sexual offences. Currently, the prevailing sexual offence laws foster an environment where the probability of offenders facing tangible real-life repercussions is extremely low(Cantley and Dietrich, 2022).

Nature of criminal behaviour in the Metaverse

Analysing criminal behaviour in the metaverse requires an understanding of the types of crimes committed in this virtual environment. For this reason, international police agencies such as INTERPOL are launching innovative metaverse initiatives to help protect communities and ensure the rule of law (Marr, 2022). Building on this, the metaverse offers many benefits to law enforcement agencies, allowing them to collect and preserve evidence at virtual crime scenes, but it can also be used to train officers to deal with real-world situations. Based on this idea, one of the unique aspects of the Metaverse is the potential immersive realism that users feel. Even though experiences in the metaverse do not have physical consequences, the psychological damage and potential trauma are far more difficult to examine (Yang, 2022). Another question that many policymakers ask is why people commit crimes in the metaverse when they do not even know the user. This is due to the anonymity and disinhibition within the metaverse, which explains why individuals choose to engage in unethical behaviour, due to a lower sense of accountability. Furthermore, the challenge of ensuring rapid accountability arises from the fast interoperability between metaverses, as criminals move freely between platforms. Accountability in the metaverse is important to ensure that users' sensitive data are handled in compliance with data protection (under the General Data Protection Regulation), which could be dangerous if individuals' data such as the location of users, behaviour patterns, and environment are shared (Sephton, 2022; Y. Wang et al., 2023). Additionally, to avoid this criminal liability and data sharing, the metaverse requires the implementation of monitoring systems. It has been shown

that more than one-third of consumers (37%) are concerned about their security and the risk of identity theft in the metaverse (Norton, 2022). The concept of pervasive surveillance, which refers to the monitoring and recording of virtual interactions, has also been reflected in criminal liability. which goal is to control and monitor the behaviour and activities of individuals who are under suspicion or acting without cause (Bibri and Allam, 2022). This is very useful as it acts as a deterrent to criminal behaviour, knowing that a person's actions are being monitored and recorded makes it less likely that individuals will engage in illegal online behaviours, as the risk of being identified and held accountable increases (Stoycheff et al., 2019).

The metaverse world derives directly from the criterion that a metaverse must provide a milieu for human culture and interaction, as is the case in the physical world. Moreover, our identities will be universally recognisable primarily through our physical embodiment (Dionisio, Burns, and Gilbert, 2013), and as Madiega et al. (2022) point out in their EU policy briefing paper, biometric technological methods are now tracking our emotions for behavioural advertising, eye trackers to measure attention in the world, and increased consumer manipulation. This monitoring is important to ensure the security and integrity of the virtual environment and protect users from malicious activity. Further, this type of monitoring can be interpreted based on governments or scientifically unsound rules and regulations (Bibri and Allam, 2022). For example, European regulators have been the most active in setting basic standards to ensure privacy and consumer protection. In the United States, however, technology companies do not face similar regulations or accountability, and this is because they are 'virtually immune' from legal liability. Goldberg (2022) argues that Meta (Facebook's recent rebrand) would not face laws that would make them liable simply because they do not exist. This highlights the problem of lack of liability and an area where there is no precedent or laws to protect users, specifically and explicitly against digital and virtual sexual assault and harassment.

Examining harms under current criminal legislation

This dilemma arises from the decentralised nature of the metaverse, where borders no longer exist. Complications arise when users interact with each other through their avatars, as altercations that would constitute a breach of real-world laws can occur within this virtual space. Considering the significant negative impact that cyber harassment often has on its victims, it is

imperative to establish a robust network of security measures to control the crime and thus address and remedy such incidents. Unfortunately, it is typically difficult to track verbal misconduct in the metaverse because events occur in real-time and some websites may not be recorded. While the legal and policy framework for the metaverse is still evolving and no meta-law has yet been created, some countries have begun to adapt existing laws to address online misconduct. For example, the United Kingdom has introduced the Online Safety Bill to ensure that online platforms have systems in place to combat illegal and harmful content, including identifying individuals behind harassing avatars (House of Commons, 2023). Further, in response to growing concerns about sexual harassment and abuse in the metaverse, policymakers and legislators have recognised the need for effective policy interventions. The EU digital ecosystem is highly fragmented, and although the digital economy is still developing in Bulgaria, Greece, and Romania (Turillazzi et al., 2023), other countries such as Norway and France are already mature and taking an important steps to gain valuable experience with virtual policing. In 2015, Norway began building an online presence with Internet patrols in each district, present in various social media, games, and streaming platforms. France also launched an initiative to establish a presence on Fortnite to allow children suffering from abuse, to share their stories (Marr, 2022). This fragmentation is costly, especially in terms of lower productivity, and it is exacerbated by the rising cost of compliance given the lack of harmonisation between states.

The Digital Services Act

A current policy response to crime in the metaverse is the Digital Services Act (DSA). Proposed by the European Commission, it aims to regulate digital platforms operating in the metaverse and address several challenges, including preventing online harm and protecting user safety (EC, 2023). Remarkably, it aims to apply the existing body of laws, regulations, and fundamental human rights to the current digital landscape, rather than creating a new legal framework (Anand and Bird, 2023). To this end, this policy works to introduce liability, transparency, and security not only in online environments, but also in services and products such as games (Bavana, 2021). And any kind of violation of the law can lead to significant fines of up to 6% of the total global annual turnover, exceedingly even the maximum penalties of the General Data Protection Regulation (GDPR) (Yakimova and Hoeglund, 2022). While this is the

main plan, the question is how to strike a balance between 1) protecting the user's security, rights and safety and, 2) combating and punishing criminal activity in the metaverse at the same time.

On the one hand, in addressing sexual abuse and harassment in the metaverse, the DSA has established clear and standardised reporting and withdrawal procedures (Micova and Streel, 2020). This is beneficial to ensure that individuals who encounter illegal content, including instances of sexual abuse, online abuse, or harassment, can easily report it and expect a timely response from platform providers, and it will assist in the immediate removal of harmful content from online spaces. In addition to banning this illegal content, metaverse providers (such as Roblox or Facebook platforms) will also be required to be highly transparent and report all of their information. The DSA provides that they must be more transparent about their content moderation policies, practises, and procedures so that governments know how they handle reports and actions against sex offenders (Pehlivan and Church, 2023). This is positive because it helps create an accountable and trusting community among users. At the same time, the European Commission (2023) is working with codes of conduct to counter the negative effects of the viral spread of illegal content and manipulative and abusive activities that are particularly harmful to vulnerable users such as children and minors. This includes implementing age verification mechanisms, adopting child-friendly policies, and ensuring the safety of minors in online environments. As a result, digital service providers need to formulate their terms and conditions in a way that children can understand to protect them from age-inappropriate and illegal content (Negreiro, 2023).

On the other hand, while the DSA is a comprehensive legal framework to address various issues related to online activities, there are still some challenges that it cannot fully address in the context of crimes such as online sexual abuse and harassment. Often, these types of unethical behaviour involve perpetrators and victims from different countries, and coordinating investigations and legal actions across borders can be challenging. The DSA should be consistent with horizontal cooperation between national authorities. According to Article 38(2), cross-border enforcement is organised by the digital services coordinator of the Member State where a digital service provider has its principal place of business or its representatives, and the coordinator is responsible for organising cross-border enforcement (Mustert and Bledoeg, 2021). In line with this goal, this is a complex issue as there is a need to ensure strong harmonisation

across borders to address and prevent any online abuse, as there are differences in the way national laws are developed (Gabriele, 2023). While the DSA focuses on creating more security and accountability in the digital space, security itself includes protection from digital violence, which is not given enough attention in the policy. In addition, it may not comprehensively cover the provision of psychosocial support and potential resources for victims of sexual abuse, online abuse, and harassment. There is a need for holistic support systems that go beyond legal and technical measures to address the psychological impact and well-being of those affected by these crimes. And the only solution they offered was that online platforms, including social media and marketplaces, must be the ones proposing measures to protect users from illegal content.

In addition, VLOPs (very large online platforms) must analyse systemic risks every year and conduct a risk mitigation analysis. This requires continuous monitoring to reduce risks related to sexual abuse and harassment, which usually have negative impacts on fundamental rights, public safety, gender-based violence, and minors, and thus consequences for users' physical and mental health (Heywood, 2022). For these reasons, the DSA should have access to any kind of platform support that allows them to quickly report, immediately review and delete illegal content. The final decision on illegal content must be left to the courts under the rule of law (Hate Aid, 2022). In addition, the DSA should continue to establish rules that ensure transparency and access to information. This is of utmost importance given the great asymmetry of information between digital platforms and regulators. In addition, expanding transparency requirements for the metaverse can ensure that users and the public have greater insight into platforms' practises (Maroni, 2023). This could include disclosure of algorithms and moderation policies that can assess compliance and support proceedings in the criminal justice system by providing transparent reports and independent oversight mechanisms (Article 13).

Further policy improvements

Overall, this policy has demonstrated clear guidelines and procedures that are consistent and effective in reporting and punishing sexual abuse. Nevertheless, some further developments can be addressed. First, better collaboration between digital providers and law enforcement could improve the investigation and prosecution of sexual abuse cases in this virtual world. This collaboration could include establishing dedicated communication channels or providing the

necessary resources and training to ensure cooperation. In addition, these companies should be able to deploy proactive detection technologies that can identify patterns, keywords, and behaviours that might indicate online harassment between avatars. They could implement systems such as machine-learning algorithms and AI-driven systems (Senftleben, 2022) to automatically flag and remove harmful content and harmful individuals, reducing the burden on individuals who sometimes fail to report such incidents. In addition, it could be beneficial to introduce stricter penalties and accountability (Suzor, Seignior, and Singleton, 2017). Each country's legislation should include more severe penalties for both digital providers and the perpetrators themselves to combat this type of crime. In addition, as mentioned in the report, relevant organisations should take initiatives to support victim assistance and rehabilitation programmes to provide support, counselling, and resources to victims who have been sexually abused online. Balancing these various considerations is crucial to the effectiveness and legitimacy of the Digital Services Act in combating criminal activity in the metaverse while respecting individual rights and promoting innovation.

.

LIST OF REFERENCES

Abbott, R. (2022) *Research Handbook on Intellectual Property and Artificial Intelligence*. Cheltenham, UK: Edward Elgar Publishing. Available at: https://doi.org/10.4337/9781800881907.

Anand, R. and Bird, B. (2023) 'The Digital Services Act and Vulnerability: How Vulnerability is Defined by Digital Regulations in the EU', *Irish Law Times*, 41(9), pp. 135–140.

Bavana, K. (2021) 'Privacy in the Metaverse', *Jus Corpus Law Journal*, 2(3), pp. 1–11.

Bibri, S.E. and Allam, Z. (2022) 'The Metaverse as a virtual form of data-driven smart cities: the ethics of the hyper-connectivity, datafication, algorithmization, and platformization of urban society', *Computational Urban Science*, 2(1), p. 22. Available at: https://doi.org/10.1007/s43762-022-00050-1.

Bovenzi, G.M. (2023) 'MetaCrimes: Criminal Accountability for Conducts in the Metaverse', in *Companion Proceedings of the ACM Web Conference 2023*. New York, NY, USA: Association for Computing Machinery (WWW '23 Companion), pp. 565–567. Available at: https://doi.org/10.1145/3543873.3587535.

Cantley, B. and Dietrich, G. (2022) 'The Metaverse: A Virtual World with Real World Legal Consequences', *Rutgers Computer and Technology Law Journal*, 49(1), pp. 1–25.

Chalmers, D.J. (2022) 'What Should be Considered a Crime in the Metaverse?' Available at: https://www.wired.com/story/crime-metaverse-virtual-reality/#:~:text=Actions%20in%20virtual%20worlds%20will,virtual%20realities%20as%20genuine%20realities. (Accessed: 12 March 2023).

Coillet-Matillon, P. (2022) 'The Criminal Police is entering the Metaverse'. Available at: https://incyber.org/en/criminal-police-is-entering-metaverse/ (Accessed: 17 April 2023).

Dionisio, J.D.N., Burns, W.G. and Gilbert, R. (2013) '3D Virtual Worlds and the Metaverse: Current Status and Future Possibilities', *ACM Comput. Surv.*, 45(3). Available at: https://doi.org/10.1145/2480741.2480751.

European Commission (2023a) 'Questions and Answers: Digital Services Act'. Available at: https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348 (Accessed: 16 May 2023).

European Commission (2023b) 'The Digital Services Act Package'. Available at: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package (Accessed: 16 May 2023).

European Parliament (Council of the European Union) (2022a) *Digital Services Act, Article 13*. Available at: https://eur-lex.europa.eu/eli/reg/2022/2065/oj.

European Parliament (Council of the European Union) (2022b) *Digital Services Act*, Article *38*. Available at: https://eur-lex.europa.eu/eli/reg/2022/2065/oj.

Gabriele, S. (2023) 'La Unión Europea regula el Internet: Contenidos, transparencia y algoritmos en la nueva DSA', *Gabilex: Revista del Gabinete Jurídico de Castilla-La Mancha*, (44), pp. 389–478.

Haber, E. (2023) 'The Criminal Metaverse', *Indiana Law Journal* [Preprint]. Available at: https://ssrn.com/abstract=4400281.

Hate Aid (2022) 'Digital Services Act: Barely Any Protection for Victims of Digital Violence'. Available at: https://hateaid.org/en/press-release-digital-services-act-barely-any-protection-for-victims/# (Accessed: 17 May 2023).

Henry, N. and Powell, A. (2016) 'Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law', *Social & Legal Studies*, 25(4), pp. 397–418. Available at: https://doi.org/10.1177/0964663915624273.

Heywood, D. (2022) 'EC Digital Services Act agreed'. Available at: https://www.taylorwessing.com/en/insights-and-events/insights/2022/05/ec-digital-services-act-agreed (Accessed: 16 April 2023).

House of Commons (2023) 'Online Safety Bill (Government Bill)'. Available at: https://bills.parliament.uk/bills/3137.

Huggett, J. (2020) 'Virtually Real or Really Virtual: Towards a Heritage Metaverse', *Studies in Digital Heritage*, 4(1), pp. 1–15. Available at: https://doi.org/10.14434/sdh.v4i1.26218.

Huynh-The, T. *et al.* (2023) 'Blockchain for the metaverse: A Review', *Future Generation Computer Systems*, 143, pp. 401–419. Available at: https://doi.org/10.1016/j.future.2023.02.008.

Madiega, T. *et al.* (2022) *Metaverse Opportunities, risks, and policy implications*. European Parliament: European Parliamentary Reseach Service. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733557/EPRS_BRI(2022)733557_EN.pdf.

Maroni, M. (2023) '"Mediated Transparency": The Digital Services Act and the Legitimisation of Platform Power', *Helsinki Legal Studies Research Paper* [Preprint], (77). Available at: https://ssrn.com/abstract=4413531.

Marr, B. (2022) 'Policing in The Metaverse: What's Happening Now'. Available at: https://www.forbes.com/sites/bernardmarr/2022/11/18/policing-in-the-metaverse-whats-happening-now/ (Accessed: 10 April 2023).

McStay, A. (2023) 'The Metaverse: Surveillant Physics, Virtual Realist Governance, and the Missing Commons', *Philosophy & Technology*, 36(1), p. 13. Available at: https://doi.org/10.1007/s13347-023-00613-y.

Micova, S.B. and Streel, A. de (2020) *Digital Services Act: Deepening the Internal Market and Clarifying Responsibilities for digital services*. Centre on Regulation in Europe. Available at: https://cerre.eu/wp-content/uploads/2020/12/CERRE_DSA-Recommendations-November2020.pdf.

Murphy, S. *et al.* (2021) 'The Metaverse: The evolution of a universal digital platform'. Available at:

https://www.nortonrosefulbright.com/fr-fr/knowledge/publications/5cd471a1/the-metaverse-the-evolution-of-a-universal-digital-platform#section4 (Accessed: 15 May 2023).

Mustert, L. and Bledoeg, M. (2021) 'The DSA Enforcement Framework, Lessons Learned from the GDPR?' Available at: https://eulawenforcement.com/?p=8038 (Accessed: 15 May 2023).

Negreiro, M. (2023) *Online age verification methods for children*. European Parliament: European Parliamentary Research Service. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733557/EPRS_BRI(2022)733557_EN.pdf.

Norton, N. (2022) 'Overcoming barriers to the metaverse requires ubiquitous connectivity'. Available at: https://www.amdocs.com/insights/blog/overcoming-barriers-metaverse-requires-ubiquitous-connectivity (Accessed: 17 May 2023).

Onggirawan, C.A. *et al.* (2023) 'Systematic literature review: The adaptation of distance learning process during the COVID-19 pandemic using virtual educational spaces in metaverse', *7th International Conference on Computer Science and Computational Intelligence 2022*, 216, pp. 274–283. Available at: https://doi.org/10.1016/j.procs.2022.12.137.

Pehlivan, C. and Church, P. (2023) 'The EU Digital Services Act: A new era for online harms and intermediary liability'. Available at: https://www.linklaters.com/en/insights/blogs/digilinks/2023/february/the-eu-digital-services-act---a-new-era-for-online-harms-and-intermediary-liability (Accessed: 16 May 2023).

Pietro, R.D. and Cresci, S. (2021) 'Metaverse: Security and Privacy Issues', in *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*. *2021 Third IEEE International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS-ISA)*, pp. 281–288. Available at: https://doi.org/10.1109/TPSISA52974.2021.00032.

Senftleben, M. (2022) 'Chapter 16: Trademark law, AI-driven behavioural advertising, and the Digital Services Act: toward source and parameter transparency for consumers, brand

owners, and competitors', in. Cheltenham, UK: Edward Elgar Publishing, pp. 309–324. Available at: https://doi.org/10.4337/9781800881907.00023.

Sephton, C. (2022) 'Crime in the Metaverse: What could possibly go wrong?' Available at: https://currency.com/crime-in-the-metaverse-what-could-possibly-go-wrong (Accessed: 17 May 2023).

Singh, K. (2022) 'There's Not Much We Can Legally Do About Sexual Assault in The Metaverse'. Available at: https://www.refinery29.com/en-us/2022/06/11004248/is-metaverse-sexual-assault-illegal (Accessed: 10 April 2023).

Stephens, M. (2022) *Metaverse and its Governance*. United States: The Institute of Electrical and Electronics Engineers. Available at: https://standards.ieee.org/wp-content/uploads/2022/06/XR_Metaverse_Governance.pdf.

Stoycheff, E. *et al.* (2019) 'Privacy and the Panopticon: Online mass surveillance's deterrence and chilling effects', *New Media & Society*, 21(3), pp. 602–619. Available at: https://doi.org/10.1177/1461444818801317.

Suzor, N., Seignior, B. and Singleton, J. (2017) 'Non-consensual porn and the responsibilities of online intermediaries', *Melbourne University Law Review*, 40(3), pp. 1057–1097.

Syed Abdul, S. *et al.* (2022) 'Virtual reality enhancing medical education and practice: Brief communication', *DIGITAL HEALTH*, 8, p. 20552076221143948. Available at: https://doi.org/10.1177/20552076221143948.

Turillazzi, A. *et al.* (2023) 'The digital services act: an analysis of its ethical, legal, and social implications', *Law, Innovation and Technology*, 15(1), pp. 83–106. Available at: https://doi.org/10.1080/17579961.2023.2184136.

Wiederhold, B.K. (2022) 'Sexual Harassment in the Metaverse', *Cyberpsychology, Behavior and social networking*, 25(8). Available at: https://doi.org/10.1089/cyber.2022.29253.editorial479.

Y. Wang *et al.* (2023) 'A Survey on Metaverse: Fundamentals, Security, and Privacy', *IEEE Communications Surveys & Tutorials*, 25(1), pp. 319–352. Available at: https://doi.org/10.1109/COMST.2022.3202047.

Yakimova, Y. and Höglund, I. (2022) 'Digital Services Act: agreement for a transparent and safe online environment'. Available at: https://www.europarl.europa.eu/news/en/press-room/20220412IPR27111/digital-services-act-agreement-for-a-transparent-and-safe-online-environment (Accessed: 17 May 2023).

Yang, J. (2022) 'Crime in a Digital World: Sexual Misconduct in the Metaverse.' Available at: https://crucible.law/insights/crime-in-a-digital-world-sexual-misconduct-in-the-metaverse (Accessed: 16 May 2023).

Zima, M. (2022) 'The metaverse: virtual offences, real world penalties?' Available at: https://www.kingsleynapley.co.uk/insights/blogs/criminal-law-blog/the-metaverse-virtual-offences-real-world-penalties (Accessed: 12 March 2023).