International Journal of Education & Social Sciences (IJESS)
ISSN: 2754-2793
Vol. 5 Issue 11, November - 2024

Extended Reality (XR) And Cyber Crimes In The Metaverse: A Comparison Between India And The UK

DEEPA MANICKAM
(Assistant Professor of Law,
Tamil Nadu National Law University, Tiruchirappalli)
deepamanickam@tnnlu.ac.in

ANUSRI AR
(LL.M Business Law)
anusriar97@gmail.com

1. INTRODUCTION

The forthcoming Web 3.0 framework seeks to set up decentralized work environments and guarantees completely seamless experiences via the metaverse. The current Internet world is occupied with the Artificial Intelligence (AI) and its effective development in the cyberspace arena. All the countries initiated to invest in AI technologies to boost their economy(Tambiama Madiega, Rafał Ilnicki, 2024).The focus should be placed on the contemporary issues of Extended Reality (XR) in the metaverse virtual set-up.

The word ‘metaverse’ was coined by Neal Stephenson in 1992 with the meaning of transcendence for ‘meta’ and universe for ‘verse’. Metaverse refers to the set of virtual environments that seek to bridge the gap between our physical and virtual lives. This technology is undergoing a tremendous and upheaval. The emergence of novel developing technology like the metaverse refers to the goal of merging the various dynamic technologies like Virtual Reality (VR)(*Virtual Reality, the Technology of the Future - Iberdrola*, n.d.), Augmented Reality (AR)(*What Is Augmented Reality (AR)?*, n.d.), and Mixed Reality (MR)(*Virtual Reality vs. Augmented Reality vs. Mixed Reality - Intel*, n.d.) into a single expansive, interactive virtual world where users will be able to switch easily among multiple environments. It is not about switching into multiple environments but the immersive ambience provided by the above-mentioned sophisticated technologies and the challenges faced by the Internet users.

To improve algorithm–driven and immersive virtual reality world experience, the internet users already provide sensitive and confidential data to the websites specifically gaming platforms which increases the unprecedented level of immersion in the metaverse creating data privacy issues, deep fakes, identity thefts, and mental health hazards.

The metaverse makes children and youth increasingly exposed to the use of digital platforms and the Internet of Things (IoTs) and affects their psychological and physical wellness. The metaverse use is associated with an increased risk of mental health problems including but not limited to Anxiety issues, addiction to usage, self-harm, social distance etc., Serious metaverse-related cybercrimes among youths which include cyber bullying, sexual assault, online exploitation, privacy concerns and security breaches add to the burning oil. The recent case on virtual rape of a 16 years old girl in the United Kingdom shook the world and hence focusing on the niche area of virtual rape is significant now.

This current research article discusses further the understanding between Extended Reality (XR) and Artificial Intelligence (AI) in the metaverse in comparison between the United Kingdom and the Indian legal regime. The specific focus is laid on the UK because of the development of the legal regime on cyber laws since the enactment of Computer Abuse Act, 1990(Participation, n.d.) after tackling notable case laws R v. Thompson(*R v. Thompson, (1984) 79 Cr App R 191*, n.d.) and R v. Gold and Schifreen(*R v. Gold and Schifreen, CACD [1987] QB 1116*, n.d.). The article refrains from resolving these issues in its entirety but aims to critically analyse the problem areas in this intersection between metaverse and cybercrimes. In addition, it elaborates on the concerns about the effects of the metaverse cries and virtual rape on the victims. The article discourses on the India position on the legal issues relating to metaverse and cybercrime in the age of artificial intelligence.

2. EXTENDED REALITY (XR) AND THE METAVERSE- AN ANALYSIS

“The rise of powerful technologies such as the metaverse is making the criminal landscape increasingly complex and transnational, posing new challenges for law enforcement”

-Jurgen Stock, INTERPOL Secretary General.

The next-gen Internet, the metaverse, shapes a completely immersive, self-sufficient virtual shared space for netizens or cybernauts to play, work, and socialize. The metaverse, a cyber reality which is filled with many contemporary technologies like extended reality, blockchain, and artificial intelligence.(*Metaverse or Metaworse? Cybersecurity Threats Against the Internet of Experiences*, n.d.)

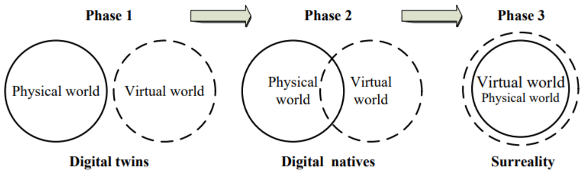

FIG. 1: Three phases of the development of the metaverse (*Metaverse or Metaworse? Cybersecurity Threats Against the Internet of Experiences*, n.d.)

To be precise, the existence of the metaverse does not require VR, AR, and MR. A Fortnite player who utilizes an avatar does not require extended reality. Nonetheless, the metaverse has bestowed a newfound significance on these technologies. An example of this can be seen in the metaverse, as conceptualized by Mark Zuckerberg, CEO of Meta,(*Metaverse or Metaworse? Cybersecurity Threats Against the Internet of Experiences*, n.d.) which comprises virtual realms accessible via extended reality. Meta's recent announcement that users will be able to access VR devices without a Facebook account has been interpreted as the company's strategy to attract subscribers from one that relies on social media to one that is preoccupied with the metaverse.(*How to Use a Meta Quest 2 or 3 without Facebook*, n.d.)

Extended reality is crucial for the development and utility of the metaverse. We argue in the metaverse Technology Framework, a recently published white paper by Centific,(pratheeksha.n, 2023) that metaverse experience layer will further develop in tandem with the emergence of additional use cases, thereby enhancing the metaverse's allure to the general public. It is an imminent development that the metaverse will permeate every aspect of our existence and seamlessly integrate itself into the tangible realm. At this juncture, extended reality becomes relevant. The user experience in the metaverse will be enhanced using extended reality-focused devices such as haptics(*HAPTIC | English Meaning - Cambridge Dictionary*, n.d.), hologram displays(*Holographic Display Technology - This Is How It Works*, n.d.), AR smart eyewear, and VR headgear("The Best VR Headset," 2024). These devices can enable a multitude of tangible services within the virtual realm and assist users in navigating the metaverse effortlessly.(pratheeksha.n, 2023)

THE METAVERSE:

The word metaverse originates from NEAL STEPHESON'S science fiction book "Snow Crash" in 1992. The term *metaverse* is a blend of two words "*Meta" and "Universe*". Neal discussed it as a logical progression from the cyberspace**.** A The metaverse is an internet-accessible virtual three-dimensional environment. In addition to engaging in collaborative activities and one-on-one conversations, users may also utilize computer-generated fictional characters. This is a simulated environment in which internet-based transactions occur involving real-world data.(Dwivedi et al., 2022)

EXTENDED REALITY(XR):

Extended reality also called XR is a concept that involves immersive technology merging the real and virtual realms. XR includes Virtual Reality, Augmented Reality, and Mixed Reality. This technology changes how users see reality, enabling them to interact with digital things seamlessly. Traditional 2D interfaces, such as those found on mobile phones and computer displays, are distinct from XR. XR technology, as opposed to conventional interfaces, transports users to an entirely new universe. This technology is expanding its application across a variety of industries at an accelerated rate. A new reality is produced by the technology's fusion of the physical and digital worlds. This is accomplished through the utilization of a variety of devices, including smartphones, tablets, Head Mounted Displays (HMDs) and sensory feedback technologies.(*Extended Reality and Metaverse: Immersive Technology in Times of Crisis SpringerLink*, n.d.)

2.1 CLASSIFICATION OF EXTENDED REALITY (XR):

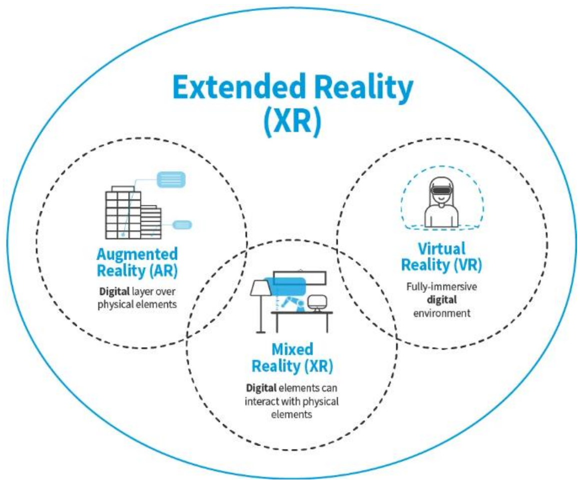

FIG 3: REPRESENTING EXTENDED REALITY (XR)(*What Is Augmented Reality (AR)?*, n.d.)

VIRTUAL REALITY (VR):

Using Virtual reality, one may become completely immersed in a computer–generated environment. Wearing an HMD blocks and sound thereby cutting the user off from their immediate surroundings. Various Haptic feedback devices and portable consoles allow users to interact with the virtual world. Playing games, the Entertainment industry, Learning, medical care and construction are just a few of many industries that make use of this technology. Because it provides a controlled environment in which users may practice virtual reality which is a great aid for training simulations.(*What Is Extended Reality (XR)? — Updated 2024 | IxDF*, n.d.)

AUGMENTED REALITY (AU):

It can be seen as an advancement and progression of Virtual Reality (VR). In addition to being an interactive experience, AU permits simultaneous user interaction with synthetic and real-world data. The technology superimposes virtual information or imagery onto the user's actual worldview; nevertheless, there is no real-time interaction between the virtual content and the physical environment. In response to the 2011 earthquake in Haiti, Crisis Commons and OpenStreetMap were implemented in AR's initial application.

The technological apparatus that superimposes virtual data into the physical environment. AR is frequently implemented in smartphone applications, that provide information about an object when the user points their device at it. Additionally, AR is being implemented in numerous sectors, including retail and tourism. AR can deliver a distinctive purchasing experience to consumers through the superimposition of Digitalized data into tangible stuff. Augmented Technology can also be utilized to inform tourists about significant historical sites and landmarks.(*What Is Augmented Reality (AR)?*, n.d.)

MIXED REALITY (MR)

A technology known as Mixed Reality (MR) combines the physical and digital worlds. MR enables the reciprocal interaction of users and digital objects in the physical world. MR is accomplished via HMD that simultaneously superimposes digital objects onto the actual world. As the image above depicts, MR is frequently implemented in sectors including architecture and real estate. MR enables architects to modify their designs before construction by providing a means to visualize them in real-world environments. Real estate is also utilizing MR to offer virtual excursions of properties.(Raghavan, 2023)

2.2 HISTORY AND EVOLUTION OF ER:

2.2.1 BETWEEN THE 1980S AND 2000

Virtual reality technology saw a significant upgrade in the 80's. VPL Research INC., in 1985 introduced 1st virtual reality gloves and glasses. Jaron Lanier one of VPL's co-founders, came up with the phrase "Virtual reality". Then, in 90's motion simulators like SEGA VR-1 appeared in arcade games. Even home VR headsets started to become more inexpensive in the mid-1990s.

In 1998, the first National Football League (NFL) match to air live on sports vision featured a yard flag, that was superimposed on the live-stream feed video. The idea was ground-breaking and other broadcasts soon followed suit with graphics overlaid across the live feed.(*History of VR – Timeline of Events and Tech Development – VirtualSpeech*, n.d.)

2.2.2 FROM 2010 TO 2020

Excluding the early 2000s due to a lack of significant advancements in extended Reality technology. (The launching of Google Street View in 2007 might be considered related to virtual reality as it enables users to virtually explore diverse locations.) Since 2010, XR technologies started to gather momentum. Notable achievements from this decade are:

Palmer Luckey who was 18 years old in 2010, designed the first version of the Oculus Rift Virtual headset. Reigniting interest in Virtual reality, the groundbreaking device used system processing power and had a 90-degree view. In 2014, FB paid close to 2 billion dollars to purchase Oculus VR, Luckey's startup after a crowdfunding promotion for the headgear had garnered $2.4 million.

FIG. 2: Oculus Rift(*History of VR – Timeline of Events and Tech Development – VirtualSpeech*, n.d.)

In 2014, Brands like Samsung and Sony announced plans to produce their brand of Virtual reality gadgets. Google unveiled its first holographic device, a cheap hologram VR gadget for mobiles, and Augmented reality spectacles, which superimpose virtual data into the physical environment and enable consumers to use programs such as mail. User reception to Google's Augmented reality spectacles was tepid, with consumers being labelled "glassholes," but Google found better success with corporate versions of Google Glass.

In 2016, Microsoft introduced the HoloLens headgear, elevating the concept of augmented reality by offering a more engaging and participatory experience, thereby coining the term "mixed reality." That year, the Pokémon GO app popularized augmented reality (AR). By the conclusion of 2016, several firms were engaged in the improvement of VR and AR experiences.(Javornik, 2016) In 2017, the IKEA Place app, released in 2017 was an early example of augmented reality in a well-known retail setting. Before buying furniture, customers may use this technology to see how it will look in their place.(*Launch of New IKEA Place App – IKEA Global*, n.d.)

In 2020, the COVID-19 pandemic compelled people to engage in virtual forms of engagement and communication. Extended reality has quickly expanded its applications throughout several sectors. The implementation of XR technology in many industries such as industry, education, healthcare, and construction.(Marr, n.d.)

2.2.3 IN THE YEAR OF 2021:

Microsoft introduces Mesh as an extension to Teams to enhance communication with an enjoyable and personalized touch. Mark Zuckerberg announced that Facebook's parent company will be renamed Meta and presented the strategy for the metaverse.(Mac et al., 2022)

2.3 The Role of Generative AI in XR

1. CREATION AND AUGMENTATION OF CONTENT

Generative AI is of paramount importance in the realm of augmented reality content creation and enhancement.

- Virtual Worlds: Generative AI can generate lifelike 3D models, textures, and animations within VR environments, thereby augmenting the level of immersion.
- Augmented reality (AR) overlays: Generative AI has the capability to produce real-time overlays that enhance the user's perspective by incorporating contextually pertinent data, including directions, object information, and historical facts.(meghnan, 2023a)

2. REALISTIC ASSETS AND ENVIRONMENT

The construction of exceptionally realistic virtual environments and assets is made possible by generative AI:

- Environmental**:** VR environments have the capability to be generated or modified in real-time in response to user interactions or empirical data, thereby offering an inexhaustible array of exploration opportunities.
- Object Generation: Generative AI contributes to the realism of XR experiences by generating genuine 3D objects, characters, and items.(meghnan, 2023b)

3. CONTENT THAT IS ADAPTIVE AND PERSONALIZED

With generative AI, XR content can be customized and adapted to specific users:

- Adaptive: Generative AI is capable of modifying narratives in XR storytelling experiences in response to user input, thereby generating distinct story trajectories for every individual user.
- Personalized Augmentation: Augmented reality (AR) applications can personalize visual enhancements and information overlays according to the preferences and context of the user.

4. TRANSLATION IN REAL-TIME AND OBJECT RECOGNITION

Generative AI augments the operational capabilities of XR through the provision of object recognition and real-time translation:

- Language Translation: The utilization of augmented reality (AR) applications to translate text in real-time enables the accessibility of foreign languages and streamlines international communication.
- Object Recognition: Generative AI has the capability to discern and furnish data pertaining to landmarks or objects within the user's field of view, thereby enhancing augmented reality-based navigation and educational experiences.

5 SIMULATION AND INSTRUCTION

Generative AI facilitates the development of training and simulation environments that are exceptionally realistic. Military and medical training can derive advantages from incorporating Generative AI-generated realistic scenarios and environments into XR simulations. XR enables designers and architects to visualize architectural designs in a virtual space that is genuine.(meghnan, 2023b)

3. CYBER CRIMES AND VIRTUAL RAPE IN THE METAVERSE-AN ANALYSIS

3.1 CYBER CRIMES IN THE METAVERSE

The metaverse being an interconnected digital and Physical environment presents distinct cyber security challenges that have the potential to affect developers, users, and organizations. Here are some of the most important cybercrimes in the metaverse:

3.1.1 DATA BREACHES AND ILLEGAL ACCESS OF DATA:

The growing quantity of confidential data poses serious risks of data breaches, illegal access, and abuse, companies in the metaverse will have complete control over their meta space, gather massive quantities of user data, and make money off it. The company that maintains free of cist the virtual world will still have the ability to gather such information from users, regardless of the existence of such realms.(*Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 2014)

3.1.2 IDENTITY THEFT AND DEEP FAKES USING ARTIFICIAL INTELLIGENCE (AI)

The users run the danger of having their online personas taken advantage of which may lead to a variety of problems including financial loss, misleading statements, and other forms of fraud. Specifically focusing on the evil twin of identity theft which is frauds using AI such as deepfakes.(Powell & Casillo, 2023) Google received nearly 30,000 URL deepfake porn complaints in 2024 (*Google Is Getting Thousands of Deepfake Porn Complaints | WIRED*, n.d.). Deep-faking top personalities from Mr Ratan Tata to Mr Narayana Murthy posed challenges to all the authenticated users.(Ojha, 2024) In India, the deep fake Rana Ayyub case increased awareness about AI technology and the threat to users' identity and privacy.(*I Was Vomiting*, n.d.)

3.1.3 CYBER-ATTACKS AND DISTRIBUTED DENIAL OF SERVICES (DDoS) ATTACKS:

Viruses, malware, and ransomware attack by cyber criminals and malicious software may disable services, prevent users or developers from gaining access and then demand ransoms to recover the access. The expansion of the metaverse may expose vulnerable infrastructure to DDoS assaults which have the potential to cause extensive disruption, because most the metaverse are stored on the cloud, they are subject to distributed denial of services.(Biswas, 2023)

3.1.4 DARKVERSE:

Dark verse is a recent terminology being given for organised crimes in the metaverse(Dwivedi et al., 2023). Child pornography and sexual assault are becoming more common in the dark verse and it is becoming more difficult to keep track of them. Dark verse also emphasises the psychological and physiological impacts of the metaverse on humans. Marketing avatars are utilised to attract consumers based on their behavioural pattern whereas, AI avatars are dangerously exploited to spread misinformation, disinformation, and invasive advertising.(Dwivedi et al., 2023)

3.1.5 SOCIAL ENGINEERING ATTACKS:

To get passwords, confidential data or any other assets, cybercriminals may employ sophisticated social engineering techniques, impersonate genuine entities, or take advantage of trust to cause phishing. With the proliferation and security flaws of smart contracts in the META, the risk of exploiting their weaknesses might result in substantial financial losses. The confidential information of users is more vulnerable to deception or unlawful access to their domains or services due to the decentralized nature of the metaverse which makes it substantially simpler for hackers, to secretly access information belonging to users(Allan, 2023). Vulnerabilities in software and hardware designs such as VR and AR devices, might leave users open to attacks.

3.1.6 INTERNAL THREATS**:**

Using HMDs poses serious dangers to online security. To begin with, head-mounted displays provide a 3D experience that cuts the user off from their real-world surroundings increasing their susceptibility to assaults since they become less aware of danger signals like heavy CPU consumption or gestures.(*Protecting against Cyber Security Threats in the Metaverse*, 2023)

3.1.7 THREATS OF INDUSTRIAL INTENET OF THINGS (IIoTs):

Hackers may organize physical assaults in advance if they have a digital replica of the place. Avatar taking over or obtaining the metaverse raw data are two ways where threats to IIoTs might occur.(Biswas, 2023)

3.2 VIRTUAL RAPE:

A virtual realm where the impossible things become possible and where the line between tangible and intangible blurs. A concept that has captured the imagination of millions, enabling them to experience interact and explore like never before. Virtual reality is changing the online gaming industry by placing consumers directly into a virtual experience. Virtual environments open opportunities for players to choose their adventures by interacting with characters in the environment or focusing on hot spots that trigger news scenes. Since players are physically experiencing the presence of characters within VR games. The idea of aggressive video games that enable real-life aggression has become a root cause. There is currently no widely acceptable legal definition of the notion still in its starting stages of open discussion.

To date, legal luminaries and cyber security experts have focused on cyber offences against women, especially on digital dating abuse and cyberbullying(Araújo et al., 2022). Virtual rape becomes a subject of legal and ethical deliberations. Virtual rape is when someone is coerced into an unwanted sexual act in a virtual setting. It brings into line the liberal theories of rape(Strikwerda, 2015). It may include touches, expose or otherwise tampering with depicted characters without their consent. Users' actions may change depending on whether they are interacting with your purely virtual world, where they take on the role of online avatars. Thus, a perfect definition would be that rape that occurs in the virtual space is functionally equivalent to that of rape occurring in a virtual environment.

3.3 VIRTUAL RAPE CASES:

3.3.1 IN 1993: THE VILLAGE VOICE:

The Village Voice by Julian Dibbell depicts the first ever virtual rape where a user graphically depicts sexual behaviours in LAMBDAMOO highlighting the concept of rape. It describes the invasion of personal space in terms of a person's physical integrity explaining that the actual person behind the screen is experiencing the impact of the activities performed on the virtual avatars(*JULIAN DIBBELL*, n.d.).

3.3.2 IN 2003: SECOND LIFE CASE:

Philip Rosedale created Second Life, a virtual environment where users can create intricate avatars with other users. According to the investigation, sexual assault between adult avatars provided a convenient platform for sexual misconduct among users.(Brenner, n.d.)

3.3.3 IN 2016: QUIVR GAME:

In QuiVR an archery-oriented online video game where a stranger avatar user began to strike her simulated chest and groin another stranger avatar began to pursue others throughout the game.(Clarke, 2022)

3.3.4 IN 2019: RAPE DAY GAME:

Virtual game called Rape Day was designed by Jake Roberts. It was processed that one can rape other users virtually and a petition was filed by Chance.org where 8000 signed to remove the game from Steam Direct.(MENAFN, n.d.)

3.3.5 IN 2022: NINA JANE PATEL CASE:

An avatar in the metaverse was sexually assaulted and gang raped by other users. The victim of virtual assault Nina Jain Patel alleges that it transpired within SIXTY SECONDS after entering in the metaverse and also photographed her and sent messages.(Dwivedi et al., 2023)

3.3.6 IN 2024:16YEARS OLD UK CHILD VIRTUAL RAPE CASE:

In 2024, the first time a virtual rape is under the investigation wing of UK Police. The girl child was playing a virtual reality game in the metaverse, and her avatar was gang raped by several male avatars. The child did not suffer any physical harm because it wasn't an attack in the physical world, but she suffered, nonetheless. It feels overwhelmingly real as it is designed to be completely immersive. The child suffered the psychological and emotional trauma of being raped.(Sales, 2024)

Online sexual assault was a factor in each of the cases. All of them included infractions that occurred in a digitally coded arena. They all showed human-controlled avatars having sexual encounters without the other avatar's knowledge or consent. It is evident from the reaction of the victims that they have gone through severe trauma and psychological injury which might consume time to recover.

Recently 33 attorney generals filed a lawsuit against Meta because in the recent past Meta has notably become a place destroying the rights of minor children and youth. The lawsuit claimed that Facebook and Instagram are responsible for 'national youth mental health crises'. This recent case raised questions on the regulatory framework of the UK Online Safety Bill.

3.4 IMPACT OF VIRTUAL RAPE ON VICTIM - PHYSICAL AND PSYCHOLOGICAL HARM:

VR has the potential to revolutionise the way people access mental health and allows consultation with Psychiatry and Psychology experts. A proper evaluation of VR's Potential health risks must take both the psychological and physiological accepts, taken into consideration when thinking about its long-term impacts on humans.(Tenaw et al., 2022)

3.4.1 Addiction

Virtual reality games have a higher potential for addiction compared to other online video games. In reality, the meta depends upon multisensory interaction which includes sight, voice, and touch. The ability of media to portray reality accurately is seen to be its most alluring feature. This may affect the children by way of anxiety, depression, and away from social gatherings.(Lee et al., 2021)

3.4.2 Psychological consequences of Cyber bullying:

Some members of the gaming community engage in hostile and discriminatory behaviour such as sex intimidation, homophobia, racial discrimination and transphobia too because they feel more comfortable doing so in virtual settings. It targets Children or adolescents who are away from family networks.(Jonsson et al., 2019)

3.4.3 Identity confusion:

A variety of avatars are available to users in the metaverse and the feeling of the embodiment may cause users to identify their avatar. In reality, people might utilize their idealized avatar-based characters as a means of escaping their undesirable personalities. The metaverse at this time might cause children and teenagers to become confused about who they are.(*Body Dysmorphic Features among Snapchat Users of "Beauty-Retouching of Selfies" and Its Relationship with Quality of Life: Media Asia: Vol 49 , No 3 - Get Access*, n.d.)

4.LEGAL REGULATORY FRAMEWORK – COMPARATIVE ANALYSIS OF UNITED KINGDOM AND INDIA**:**

Like any revolutionary technological advancement, the metaverse will give rise to unique and intricate ethical and legal concerns. The practical uses of the metaverse are expanding and changing due to advancements in technology, leading to new legal and regulatory obstacles. The metaverse is intended to be highly linked, seamless, and detached from physical location, further complicating the field of play. Users and businesses that operate in the metaverse face legal obstacles pertaining to intellectual property, jurisdiction, and privacy. Enforcing intellectual property laws, including those pertaining to copyright and trademark, within the metaverse could pose challenges due to the decentralized and virtual characteristics of the platform(*The Role of Legal and Compliance in the Metaverse*, n.d.). Furthermore, establishing ownership and authorization for the utilization of virtual assets within the metaverse could present obstacles. User autonomy regarding the collection, utilization, and dissemination of their data may render privacy an additional significant concern in the metaverse. This situation could lead to potential violation of legislation such as the GDPR of the European Union. Another legal obstacle is jurisdiction, as determining which laws apply in the borderless the metaverse may require considerable time. Furthermore, conflicts may emerge concerning the application of specific legal systems for the resolution of disputes that transpire within the metaverse along with the cyber security standards and ethical and social responsibility.(Kalyvaki, 2023)

4.1 CURRENT UK LAWS:

4.1.1 SEXUAL ASSAULT:(*Sexual_Offences_Act_2003.Pdf*, n.d.)

To commit sexual assault in England and Wales, one must have the intent to inflict sexual injury to another person and must get that person's consent before engaging in any sexual activity.In a legal context, "touching" can mean physical contact "with any part of the body," "with anything else," or "through anything," and it can also include physical contact with an item, an instrument, or even one's clothing. Users may feel another avatar's physical contact, giving the impression of actually touching a real person, using haptic touch and other metaverse technology. If the law views this touching as sexual and non-consensual, it might be considered sexual assault. On the other hand, a number of legal experts have recently voiced their doubts regarding this.

4.1.2 HARASSEMENT:

According to the Protection from Harassment Act of 1997 if their behaviour crossed "the boundary between conduct which is unattractive, even unreasonable, and conduct which is oppressive and unacceptable," then it may be deemed offensive. The possibility of using this provision to prosecute cases of domestic abuse and stalking has been voiced by certain analysts. Much as in the real world, this law might be used to criminalize cyberbullying in the virtual world.(Bliss, 2019)

4.1.3 HATE SPEECH:

The metaverse, both avatar-based and text-based communication, is now governed by hate speech rules. While these statutes are known as the Public Order Act in England and Wales, in Scotland they were passed in April 2024 as the Online Safety Act of 2023 and in Wales as the Hate Crime and Public Order (Scotland) Act 2021.(*Hate Crime and Public Order (Scotland) Act 2021 General Information Note*, 2021)

4.1.4 ONLINE CHILD SEXUAL EXPLOITATION AND ABUSE:

A number of statutes deal with matters relating to virtual reality and children, including the Criminal Justice Act of 1988, the Protection of Minors Act of 1978, the Communications Act of 2003, the Online Safety Act of 2023, the Sexual Offences Act of 2003, and the Sexual Offences Act of 2003.Whether the child is real or imagined, the "Explicit Imagery of a Child"(“Sexting,” n.d.) Act covers all sexual depictions of minors. To protect the privacy of children, the Information Commissioner's Office has issued rules that all online services must follow. Although many of these laws are meant to safeguard children, the National Society for the Protection of Children states that "it will be difficult to know which existing laws will be deemed applicable" until criminal charges are brought, as said by the NSPCC. According to the NSPCC report(*Child Safeguarding Immersive Technologies*, n.d.) on Child Safeguarding and Immersive Technologies, the UK government, regulators, law enforcement, and tech industry should "review legislation on a rolling basis to ensure that immersive environments are adequately covered," among other high-level recommendations delivered to these groups.(Parliamentary Office of Science and Technology & Brawley, 2024)

4.1.5 GDPR AND THE INTERNATIONAL CONVENTION ON COUNTERING THE USE OF INFORMATION AND COMMUNICATION TECHNOLOGIES (ICT) FOR CRIMINAL PURPOSES

FIG 5: REPRESENTING GDPR DATA PRINCIPLES(*Guide-to-the-General-Data-Protection-Regulation-Gdpr-1-0.Pdf*, n.d.)

The draft UN convention on countering the use of Information Communication Technologies (ICT) for criminal purposes will enable in future to counter the cybercrimes in an effective manner. The grey area is the draft does not have anything with regard to the extended reality or the metaverse. The existing GDPR principles are wide enough to address the existing concerns provided the XR and the metaverse fields move ahead from the nascent stages

4.2 RESOLVING THE JUSDICTION ISSUE IN CYBERSPACE:

There are a few laws in place that can serve as a foundation for establishing jurisdiction in virtual environments. The Brussels Regulation in the EU and the Federal Courts system and Venue Clarification Act of 2011(*PLAW-112publ63.Pdf*, n.d.) in the US both lay out the ground principles for how to decide who has the authority to hear cases involving parties located in different countries. Further, the Council of Europe's adoption of the Convention on Cybercrime (often called the Budapest Convention)("Council of Europe," 1981) establishes norms for international cooperation in cybercrime investigations and prosecutions. The case of Bragg v. Linden Research, Inc.(*Bragg v. Linden Research, Inc.,487 F.Supp.2d 593 (E.D. Pa. 2007)*, n.d.) is a prime illustration of jurisdiction in the metaverse. This case required the United States (U.S.) District Court for the Eastern District of (Pennsylvania) to resolve if it has the authority to handle a disagreement over Second Life virtual property. Despite the geographical separation of the parties and the monetary worth of the virtual property in question, the court determined that it has jurisdiction over the matter.(Dougherty, 2008)

Legislation pertaining to jurisdiction in the metaverse is presently in the developmental stages. The complexity of jurisdiction in the metaverse originates from the fact that virtual communities and worlds can transcend national boundaries and engage with numerous legal systems. When talking about jurisdiction in the metaverse, may refer to the authority or judicial system's power to control as well as execute rules in virtual worlds to reduce cybercrimes.(Kalyvaki, 2023)

4.3 CURRENT INDIAN LAWS

4.3.1 BHARATIYA NYAYA SANHITA,2023

Sexual harassment in virtual reality (VR) can be considered a criminal violation since it is carried out through a specialized technological media, making it a subset of internet harassment. This means it might be subject to the BNS and IT Act's authorities. Section 77 of the BNS deals with stalking, while section 78 deals with insults to women's modesty. However, neither clause particularly tackles online abuse that women encounter. These harassments may be covered under the "transmit" requirement of the IT Act as they occur in real time on screen and are thus considered visual pictures.(*Is India's Legal Framework Ready to Deal with Sexual Violence in Virtual Reality?*, 2024)

4.3.2 THE INFORMATION TECHNOLOGY ACT 2000:

The IT Act 2000 is specialized legislation that deals with electronic communication and technology. Provisions like Section 66E, which deals with the violation of privacy by transmitting, capturing, and publishing the image showing a person's private area, can be used to prosecute crimes committed in virtual realilty.(*Section 66E: Punishment For Violation Of Privacy | The Information Technology Act, 2000*, n.d.) Because the metaverse functions similarly to other communication mediums in that it allows users to exchange information and data via linking persons all over the globe, this space may be utilized by victims of privacy violations to seek protection. You can also seek protection under Sections 67(publishing and transmission of obscene and lascivious materials),(*Section 67 in The Information Technology Act, 2000*, n.d.) 67A (transmission or publication of sexually explicit activities or behaviour involving participation of minors),and 67B (transmission or publication of any other section). The Information Technology Act of 2000 offers the most robust legislative protection against cybercrime as the majority of illicit activities in the virtual world occur through electronic methods.

The primary goal of the IT Rules, which were established in 2021 by the Ministry of Communications and Information Technology, was to protect consumers from various forms of dangerous material. Data security, portability, accuracy, choice, consent, and disclosure are all obligations that the organization must fulfil by following certain technical and architectural guidelines.(*Metaverse: Legality & Regulatory Concerns In India - Fin Tech - Technology - India*, n.d.)

4.3.3 DIGITAL PERSONAL DATA PROTECTION ACT 2023

Justice K.S. Putt swamy (Retd.) Amr v. Union of India & OR's (2017) is an Indian case that lays forth the right to privacy. This right will be governed by the Digital Personal Data Protection Act as of 2023.When the digital avatar's privacy is compromised, it could be important to look into the Digital Personal Data Protection Act as well.(*Is India's Legal Framework Ready to Deal with Sexual Violence in Virtual Reality?*, 2024) The renders powerful tool to the data principals to erase and rectify the inaccurate personal data. Right to privacy is the intricate part of the fundamental right thus protecting the digital identity of the data principals.(K.S.Puttaswamy & v, 2012) In the recent case of Aardhya Bachchan on right to be forgotten specifically moved the ambit of the privacy right to the next level(*Aaradhya Bachchan: Experts Believe Delhi HC Judgement in Aaradhya Bachchan Case Will Ensure Privacy of Children - The Economic Times*, n.d.). In the case of *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos, Mario Costeja González,* European Court cited the Directive 1995/46/EC making netizens to de-index their personal data from search engines and browsers, if they feel inappropriate(*Google Spain SL and Google Inc v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González*, 2014). This in turn minimises the commercial exploitation of the processed data and protects digital identity of the data principals.(Section 12, Digital Personal Data Protection Act, 2023, n.d.) Ultimately, digital identity in the metaverse presents intricate legal and ethical challenges, including those related to anonymity, accountability, and privacy. It is crucial to address these concerns and provide solutions that safeguard individuals' rights and privacy while also enhancing accountability and security in the metaverse.(Parliamentary Office of Science and Technology & Brawley, 2024)

5.RECOMMENDATIONS AND CONCLUSION

A multi-faceted approach is required to the hazards created in the metaverse. The development of the metaverse based industry standards and guidelines, which encourage uniformity and equity across various virtual environment also require close cooperation with other groups and cyber security stakeholders to resolve the cybercrimes in the metaverse. Particularly, public-private partnerships are encouraged.

5.1 LEGAL FRAMEWORK WITH CYBER SECURITY STANDARDS:

Another possible solution is to work together as a community as a government and profit-making companies to build a self-regulatory framework for the metaverse, this might be done with the assistance of legal and technological professionals. A new set of rules and regulations for the data Privacy, IPR, sexual assault and harassment that are specific to the Meta technology. For data privacy, the emerging technologies for biometric data authentication and psychological analysis do not promote methods of collecting and profit from personal info that violate users right to privacy. Well-efficient industry standards should be brought in to prevent digital financial crimes.

The existing domestic criminal laws, cyber security, and cyber laws are to be tuned to the contemporary technologies to evade online sexual harassment, child abuse, and exploitation. Need for international cooperation is recommended to address the metaverse cybercrimes.

5.2 RESOLVING THE JURISDICTION CONFLICTS

The metaverse blurs geographical boundaries. People from different countries can play the same VR game. So, the policy makers have to decide which law enforcement agency has jurisdiction over which incident and to punish the offenders. Domestic laws must be tightened technologically to nab a cybercriminal who commits crimes on the metaverse. Innovative policy measures should be introduced to address the concerns.

5.3 PREVENTION OF VIRTUAL ABUSE AND PROTECTION OF MENTAL HEALTH

Though meta introduces the personal boundary, which is away from strangers, the platform should take precaution to ensure that the users are adequately onboarded by completely clarifying and showing their ability to use these safety features in an emergency. Cyberspace when it comes to harassment and threats isn't always a secure place for users. Bad behaviours and harassment of other avatars will be within an avatar-based characters. Because of this it is necessary to provide the avatar a legal identity in order to establish a connection between the avatar in the meta platform and the user behind. It is imperative that law Policy makers establish regulation to safeguard children and adolescent's users from any damage, and paediatric psychologists should stay ahead of this digital shift in order to comprehend the millennial generation and make the most of technology to offer the best alternatives.

5.4 MANDATORY ADVANCED TRAINING AND AWARENESS PROGRAMMES TO THE STAKEHOLDERS

Every democratic country should advise and conduct advanced technical training to work on the frontline at regular intervals. Consistent awareness programmes are to be engaged for all the stakeholders of cyber laws and the cyber security arena.

5.5 INTERNATIONAL COOPERATION AND FRONTLINE POLICING

International cooperation is encouraged and Conventions like Budapest and the UN Convention to combat ICT should be signed and ratified by all countries to uphold the protection of data and privacy of their internet user citizens. To be precise, the lives of young children should be protected through the international cooperation principle and INTERPOL is to be strengthened and equipped to handle all these transboundary crimes. The interested people should also be trained by the countries for frontline policing to combat and evade meta crimes focusing on virtual rapes.

5.6 CONCLUSION

In the given research paper, the authors have presented an in-depth analysis of the multi-faceted metaverse and its history, privacy and security threats. Furthermore, the relationship between Artificial Intelligence (AI) and Extended Reality (XR) has been elucidated. The converging points between AI and XR have been reviewed to analyse the role of generative AI in XR. Specifically, perspectives of the UK and Indian regime where focus on cybercrimes on in the metaverse and its impacts on Internet users. Though the UK progressed towards framing regulatory framework in preventing cybercrimes notably virtual rape in the metaverse. In India, unlike in the case of the UK, the current regulatory framework is not equipped to discuss the cybercrimes in the metaverse. Furthermore, there are little to no judicial decisions on the intersecting point between cybercrimes and metaverse, lays down the indispensable need of legal regulatory framework to address the metaverse crimes and virtual rape offence. Emphasis has been laid on the physical and psychological impacts of virtual rape of children in the metaverse. The current research sheds light on an unexplored area of virtual rape and inspires more research in this area to evade metaverse crimes in future. Hence, we can make Metaverse a safe and secure place for all users if the regulation is strengthened and accurately implemented.

References:

[1] Araújo, A. V. M. de, Bonfim, C. V. do, Bushatsky, M., & Furtado, B. M. A. (2022). Technology-facilitated sexual violence: A review of virtual violence against women. *Research, Society and Development, 11*(2), Article 2. https://doi.org/10.33448/rsd-v11i2.25757

[2] Avornik, A. (2016, October 4). The mainstreaming of augmented reality: A brief history. *Harvard Business Review*. https://hbr.org/2016/10/the-mainstreaming-of-augmented-reality-a-brief-history

[3] Biswas, J. (2023, April 27). *Metaverse and its cyber security and legal complications*. The420CyberNews. https://www.the420.in/metaverse-and-its-cyber-security-and-legal-complications/

[4] Bliss, L. (2019). The Protection from Harassment Act 1997: Failures by the criminal justice

system in a social media age. *The Journal of Criminal Law, 83*(3),217-228. https://doi.org/10.1177/0022018319829262

[5] Brenner, S. W. (n.d.). *Fantasy crime: The role of criminal law in virtual worlds* (Vol. 11).

Child safeguarding immersive technologies. (n.d.).

[6] Council of Europe. (1981). Convention for the protection of individuals with regard to automatic processing of personal data. *International Legal Materials, 20*(2), 317–325. https://doi.org/10.1017/S0020782900032873

[7] Dwivedi, Y. K., Hughes, L., Baabdullah, A., & others. (2022). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice, and policy. *International Journal of Information Management, 66*, 102542. https://doi.org/10.1016/j.ijinfomgt.2022.102542

[8] Dwivedi, Y. K., Kshetri, N., Hughes, A., & others. (2023). Exploring the Darkverse: A multi-

perspective analysis of the negative societal impacts of the metaverse. *Information Systems*

Frontiers,25(5), 2071–2114. https://doi.org/10.1007/s10796-023-10400-x

[9] *Extended Reality and Metaverse: Immersive Technology in Times of Crisis (n.d.).*

SpringerLink.https://link.springer.com/book/10.1007/978-3-031-25390-4

[10] Is India's legal framework ready to deal with sexual violence in virtual reality? (2024, January 5). *TheLeaflet*. https://theleaflet.in/is-indias-legal-framework-ready-to-deal-with-sexual-violence-in-virtual-reality/

[11] Mac, R., Frenkel, S., & Roose, K. (2022, October 10). Skepticism, confusion, frustration: Inside Mark Zuckerberg's Metaverse struggles. *The New York Times*. https://www.nytimes.com/2022/10/09/technology/meta-zuckerberg-metaverse.html

[12] Meghnan. (2023a, August 2). Generative AI in extended reality. *Persistent Systems*. https://www.persistent.com/blogs/a-new-frontier-exploring-the-intersection-of-generative-ai-and-extended-reality/

[13] Ojha, S. (2024, March 13). Nine well-known personalities who were victims of deepfake videos. *Mint*. https://www.livemint.com/news/india/from-ratan-tata-sachin-tendulkar-to-madusudan-kela-9-well-known-personalities-who-were-victims-of-deepfake-videos-

[14] Parliamentary Office of Science and Technology, & Brawley, S. (2024). What is the metaverse and what impacts will it have for society? *Parliamentary Office of Science and Technology.*https://doi.org/10.58248/PB61

[15] R v. Gold and Schifreen, CACD [1987] QB 1116.

[16] R v. Thompson, (1984) 79 Cr App R 191.

[17] Raghavan, R. (2023, April 25). What is extended reality (XR) and how is it changing the world? *Acowebs*. https://acowebs.com/what-is-extended-reality-xr/

[18] Strikwerda, L. (2015). Present and Future Instances of Virtual Rape in Light of Three Categories of Legal Philosophical Theories on Rape. *Philosophy & Technology,* 28(4), 491–510.

https://doi.org/10.1007/s13347-014-0167-7

[19] The role of legal and compliance in the metaverse. (n.d.) *McKinsey Company.* https://www.mckinsey.com/featured-insights/in-the-balance/the-role-of-legal-and-compliance-in-

the-metaverse

[20] Wang, Y., Su, Z., Zhang, N., Xing, R., Liu, D., Luan, T. H., & Shen, X. (2023). A Survey on Metaverse: Fundamentals, Security, and Privacy. *IEEE Communications Surveys & Tutorials*,

25(1), 319–352. https://doi.org/10.1109/COMST.2022.3202047

11710307982420.html