Humanities & Social Sciences Communications

ARTICLE

https://doi.org/10.1057/s41599-024-04266-w OPEN

Identity, crimes, and law enforcement in the Metaverse

Hua Xuan Qin[1], Yuyang Wang[1] & Pan Hui[1,2,3]✉

The recent Metaverse technology boom in major areas of the public's life makes the safety of users a pressing concern. Though the nature of the Metaverse as a geographically unbounded space blending the physical and the virtual presents new challenges for law enforcement and governance. To tackle these, this paper supports the establishment of a unified international legal framework. Specifically, from a law enforcer's perspective, it provides the first comprehensive discussion in the past five years on legal concerns related to identity, various types of potential crimes, and challenges to unified law enforcement in the Metaverse based on prior incidents.

[1] The Hong Kong University of Science and Technology (Guangzhou), Guangzhou, China. [2] The Hong Kong University of Science and Technology, Kowloon, Hong Kong. [3] University of Helsinki, Helsinki, Finland. ✉email: panhui@ust.hk

Introduction

Consider two scenarios: (1) a child is sexually assaulted by several strangers in the physical ('real') world, and (2) a child's **avatar**, their digital representation (Lee et al., 2021), is sexually assaulted by the avatars of several online strangers in a virtual space. As the definition of sexual assault traditionally requires "physical touching", various countries would consider (1) a crime but might be more divided over (2). Some argue that "psychological trauma" from (2) is similar to that of (1), suggesting that emotional harm alone should be enough for prosecution (Camber, 2024). Such a disconnect between law and technology is a source of concern as we head toward more immersive virtual worlds, more realistic computer-simulated community environments (e.g., Horizon Worlds (Meta, 2023)), and the creation of the Metaverse (Bellini, 2024; Gómez-Quintero et al., 2024).

Initially a science-fiction concept from Neal Stephenson's 1992 novel *Snow Crash* (Stephenson, 2022), the **Metaverse** is commonly considered to be a yet-to-be-realized augmentation of the Internet, a space unbounded by time and geographical borders (Ning et al., 2021) where the physical world and different virtual worlds co-exist (Dobrygowski et al., 2024; Gómez-Quintero et al., 2024) through physical devices allowing access (e.g., smartphones and headsets (Wang et al., 2023)), extended reality technologies providing different levels of immersion (e.g., for virtual reality and augmented reality), blockchains (digital ledgers) supporting economic and legal systems by recording transactions, and artificial intelligence (AI) automating decentralized governance (i.e., rule by the 'people' with no central authority) (Lee et al., 2021) and personalizing to user needs (Qin and Hui, 2023; Soliman et al., 2024; Wang et al., 2024b). Through avatars (e.g., 3D/2D visuals of humans or non-humans resembling users or not), users can interact with environment objects or computer-controlled digital entities, such as AI-powered avatars (Lee et al., 2021).

As the Metaverse would be built upon the physical world, it could augment its offenses through technologies (Marshall and Tompsett, 2024) in terms of (1) the number of victims and of (2) the geographical spread (Brenner, 2008). An example for (1) is the simultaneous virtual sexual assault of several users' avatars through hacking, which occurred in LambdaMOO, an early text-based virtual world (Dibbell, 2005), and could be increasingly more traumatizing with advances in computer graphics and immersive technologies (Gómez-Quintero et al., 2024). For (2), harmful content could be instantaneously transmitted anywhere through the Internet, potentially causing worldwide instability, as explored in *Snow Crash* (Stephenson, 2022). As the Metaverse would be the place where 25% of the population will spend at least one hour per day by 2030 (Bellini, 2024), this leaves many opportunities for such offenses (Collard, 2022).

Unfortunately, the law has yet to keep up with the virtual. **Law** is a system of rules (laws) enforced upon members of a society to ensure its stability (Brenner, 2008; Von Ihering, 2009) and its survival (Harari, 2018). As the virtual only started to exist recently, many societies' laws still focus on the more physically tangible (e.g., physical harm on a victim) to decide whether to criminalize an act as a **crime**, a punishable breach of the law. This focus might not properly reflect the impact of acts occurring in virtual worlds (Bellini, 2024; Brenner, 2008; Weber, 2015), potentially encouraging a surge in criminal activities (Gómez-Quintero et al., 2024). Given the industry (Heath, 2021) and governments' (Feng, 2024) plans for the Metaverse and the growing number of incidents in existing virtual worlds (Bellini, 2024; Marr, 2024; Nix, 2024), a suitable legal framework needs to be established with urgency. To fulfill the vision of a boundless Metaverse and facilitate the investigation, a legal framework would need to be international, but existing legal measures (Bond, 2022) vary across geographical jurisdictions (areas with different sets of laws, such as countries). Recently, the International Criminal Police Organization (INTERPOL) highlighted the importance of international collaboration (INTERPOL, 2024a). However, no international legal framework exists yet.

As the Metaverse has yet to exist and laws are shaped by real-life cases (Guillaume, 2011; Weber, 2015), our work aims to inform future debates on the nature of such an international legal framework by leveraging the practical relevance of speculation grounded in theory and evidence from the present (Oulasvirta and Hornbæk, 2022) through incidents from existing virtual worlds (prototypes of the Metaverse (Brenner, 2008)), cyberspace (Internet as an environment (Weber, 2015)), and science-fiction (examination of future technology (Sueur et al., 2024)). Structurally, we discuss the impact on society of how identity is defined (section "Identity"), the definition of a crime in the Metaverse (section "Crimes"), and law enforcement concerns, including governance and ethical implications (section "Law enforcement"). To the best of our knowledge, existing works only explore technical measures without bridging law and technology (Wang et al., 2022), do not cover both different potential crimes and governance issues as broadly (Bellini, 2024; Cheong, 2022; Gómez-Quintero et al., 2024; Goldberg and Schär, 2023; Malhotra, 2023; Marshall and Tompsett, 2024; McStay, 2023; Yang, 2023a), and/or are not as recent (past five years), not as accurately reflecting the impact of state-of-the-art technologies (e.g., (Brenner, 2008)).

Identity

Identity is a subjective construct made of attributes across various domains that distinguishes individuals from each other (Banaeian Far and Hosseini Bamakan, 2023; Burrows et al., 1990; Dobrygowski et al., 2024). In the physical world, these can cover one's name, cultural heritage, professional roles, age, gender, nationality/citizenship (their relationship with a specific geographical jurisdiction (The Editors of Encyclopedia Britannica, 2023)), hobbies, and ethnicity among others. Identity in the Metaverse, the "Metaverse identity", would be an extension of this physical-world identity in three layers (Dobrygowski et al., 2024): **Representation**, personal, social, and role information on identity through a combination of avatars, pseudonyms, online behavior, and other forms of digital expressions, **Data**, knowledge about identity generated by hardware and software supporting the Metaverse or the description of identity through digital footprint, the trail of data left behind, and **Identification**, authentication information, such as government-issued personal identifier (ID) numbers, usernames, passwords, and even identifying biometrics, data about one's body (e.g., fingerprints and voice) (Wu and Zhang, 2023).

These layers can allow individuals to establish validity legally and psychologically (Wu and Zhang, 2023). From a legal perspective, identity determines one's rights and duties (Al Tamimi, 2018) within a jurisdiction—responsibility for crimes, punishment and compensation (e.g., financial compensation for sexual assault (Government Digital Service, 2024)), and influence on decision-making (e.g., voting rights; section "Governance"). From a Representation layer, one's expression could incite others to report them for a crime (e.g., unwarranted sexually suggestive speech or behavior). Technologies, such as AI, could also automatically generate reports based on information from the Data layer (Wang et al., 2022). The Identification layer could provide information that influences prosecution, such as the chronological age (the time elapsed since birth (Merriam-Webster, 2024a), the "actual" age) for diminished punishment for younger individuals.

From a psychological perspective, the Metaverse identity could affect perceptions about oneself and others with three major legal implications. Firstly, when using a virtual body, such as an avatar from a first-person perspective (Bellini, 2024), individuals might develop a sense of embodiment, the feeling of being inside the virtual body (Genay et al., 2022; Guy et al., 2023; Yang et al., 2024). Depending on how immersive the technology is (e.g., how simultaneously the virtual body moves with the physical one and how vivid stimuli are) and individual differences (as seen with LambdaMOO (Brenner, 2008)), the individual might psychologically experience harm in the same way they would in the physical world (Bellini, 2024; Repetto and Riva, 2024). As embodiment through avatars can affect sensations of pain (Genay et al., 2022), the virtual could even influence physical health. These support the harm of certain virtual acts (e.g., section "Virtual sexual assault").

Secondly, embodiment can lead to identity confusion, where the individual can no longer tell apart their physical-world and virtual-world identities. Idealized Representation (e.g., avatar appearance) can make individuals, especially children and adolescents, pursue unrealistic beauty and lifestyle standards (Dobrygowski et al., 2024; Kim and Kim, 2023). Identity confusion can also encourage harmful behavior in the physical world if the individual can no longer tell apart the consequences of their actions (Yang et al., 2024) (e.g., aggressive behavior after playing a virtual reality game (Kim and Kim, 2023)). On the other hand, disconnectedness between one's identity in the virtual and in the physical from greater freedom to conceal one's physical-world identity (e.g., avatars that do not look nor sound like them (Rashik et al., 2024) or hidden legal name) could lead to less commitment toward the greater good through diminished sense of accountability (Lapidot-Lefler and Barak, 2012; Suler, 2004), perceived diminished risks of being caught for crimes (Gómez-Quintero et al., 2024), and mistrust (Wu and Zhang, 2023; Xu et al., 2024). Though limiting concealment might deprive the individual of the freedom to explore without fear of being judged, of positive cognitive and social outcomes (Xu et al., 2024), and might discourage individuals from joining the Metaverse (solutions in section "Ethical implications and other challenges during law enforcement").

Thirdly, Representation information can affect how one is perceived by others. If customization is limited, stereotypes could be perpetuated in the Metaverse (Dobrygowski et al., 2024), encouraging harm toward certain groups (Bellini, 2024). An example is the stereotypical portrayal of avatars based on gender. Historically, many video games have male characters who appear muscular and violent and female characters who appear in revealing clothes, leading to harassment (Bellini, 2024). While this could be regulated, the law could also ensure that service providers offer enough non-stereotypical choices for Representation, from gender to ethnic groups (Dobrygowski et al., 2024).

How an individual's identity is defined by law in the Metaverse can thus impact society's stability directly, through the enforcement of the law, and indirectly, by affecting perceptions. Along with individual humans, two other groups might need definitions of their identities as legal persons, entities that have rights and duties under the law (Law and Martin, 2014): organizations (e.g., service providers) and computer-controlled digital entities. As organizations are already considered legal persons in the physical world, similar laws could apply in the Metaverse (Cheong, 2022). Computer-controlled entities are the subjects of more heated debate (section "Identity of AI and other computer-controlled entities").

Identity of AI and other computer-controlled entities. AI is a technology that aims to simulate human cognitive processes (Abbott and Sarch, 2024), such as the detection of faces (Ali et al., 2021) and speech (Malik et al., 2021), the classification of law enforcement data, and the generation of 'original' content (generative AI), from conversation responses for chatbots to 3D avatar visuals (Feuerriegel et al., 2024). All these could contribute to essential use cases in the Metaverse, such as AI-powered avatars that could interact in a human-like way with users for customer service (Kato et al., 2022). Though, by simulating humans, AIs could replicate their harmful behavior, such as making wrong decisions during law enforcement (Soliman et al., 2024), creating offensive content (BBC, 2024), and affecting a human's mental health (Inaba et al., 2024) negatively as seen with the suicide of a man after conversing with an AI chatbot (Xiang, 2023). This requires examination of the criminal liability of AI, its responsibility for a crime. We first review the purpose of laws then consider different views.

Laws ensure stability through a balance between the costs to society of not criminalizing and criminalizing an act (Weber, 2015). Main goals for punishing a perpetrator are incapacitation (limiting their ability to commit more crimes, e.g., through imprisonment), deterrence (discouraging the perpetrator or others from committing more crimes) (Gómez-Quintero et al., 2024), and rehabilitation. Punishment and compensation should ensure fairness for both the victim, through psychological satisfaction, and the perpetrator, through proportionality to the crime's severity (Abbott and Sarch, 2024; Hakan Kan, 2024).

Arguments against recognizing AI as a victim and/or perpetrator mainly focus on the impracticality of our current society and AI's lack of necessary human-like capabilities. For the former, recognizing AI could raise debates about other rights (Marshall, 2023), such as whether using AI is a form of slavery (Hakan Kan, 2024), limit the freedom of humans (Abbott and Sarch, 2024), and lead to loopholes (Bryson et al., 2017). For the latter, AI systems are believed to lack the emotional capabilities that make humans experience the intended consequences of compensation and punishment, have debated ownership of assets (Barbosa, 2024; Lima et al., 2021; Sueur et al., 2024), which make them less able to compensate, and lack intent to commit harm, which, according to many laws, makes them instruments instead of perpetrators. The human guardians, such as the developers or other users, can be responsible (Hakan Kan, 2024). Many ambiguities surround proof of culpability as it depends on the definition of whether a "reasonable person" could have foreseen the consequences of an act (Hallevy, 2024). This is debatable given the unpredictability of AI algorithms (Montagnani et al., 2024; Padovan et al., 2023; Soliman et al., 2024), which can automatically adjust themselves (El Naqa and Murphy, 2015). For instance, as AI models might not accurately generate what is being asked, debates could surround whether a user accidentally generated illegal content, such as virtual child pornography (section "Sexual ageplay and child pornography"), and how responsible the developers should be, such as for the design of filters for pornographic content.

On the other hand, many support the recognition of AI as compensating or punishing it could deter other humans from getting used to harmful acts (Abbott and Sarch, 2024) by preventing identity confusion (section "Identity"), resolving ambiguities regarding the culpability of humans (Doomen, 2023; Sueur et al., 2024), and vindicate the victims (Danaher, 2016).

Laws and research have explored measures to reach a mediation. They include restrictions on AI use depending on risks (European Parliament, 2024), compensatory measures, such as compensation funds and insurance schemes (Barbosa, 2024; Casado, 2024; Vellinga, 2024), and innovations in AI design, such as AIs that can explain themselves (Padovan et al., 2023) to

diminish ambiguities on culpability or that can learn about moral behavior through rewards and punishments (Li et al., 2024; Noothigattu et al., 2019). To solve compensation issues, AIs could be trained to see financial loss as punishment and gain, as reward—much like humans. Though the definition of moral behavior for an AI could come with ambiguities, as seen in science fiction writer Isaac Asimov's short story "Liar!" (Asimov, 2004), where a humanoid robot capable of conversation, similar to an AI-powered chatbot avatar, the Metaverse, is programmed such that it should not 'harm' humans. When a user asks the robot whether her crush loves her back, the robot gives an affirmative answer, regardless of the truth, because it perceives that another answer would harm the user emotionally. While this brings joy to the user in the short term, when she discovers the truth, she suffers different emotional harm. Disclosing the truth could prevent later disappointment, but it challenges AI capabilities in determining the truth (McIntosh et al., 2024) and has privacy implications (e.g., the AI would need the crush's personal data). Alternatively, how experts respond in emotionally difficult situations could be studied (e.g., conversations about end-of-life care (Balaban, 2000)).

Crimes

Two types of crimes could exist in the Metaverse: "cybercrimes", acts already criminalized by many jurisdictions despite some nuances (Iu and Wong, 2023), and "fantasy crimes", acts that have generally not been criminalized but whose physical-world counterparts generally are (e.g., virtual sexual assault). Their criminalization is contested mainly due to a historical focus on proving physically tangible harm. However, current debates suggest that, as we move toward a world that blends the physical with the virtual (Metaverse), a re-assessment of the costs and benefits of criminalizing fantasy crimes is needed, possibly with more weight on the psychological impact (section "Introduction).

To inform criminalization, this section provides insights into cybercrimes (section "Cybercrimes") and fantasy crimes (section "Fantasy crimes) by covering existing cases, hypothetical scenarios, and different laws across jurisdictions. Existing cases and laws could provide insights into the costs to society in resolving differing views for an international framework. Though they need to be extended by hypothetical scenarios because the society we know now might be vastly different from our envisioned society integrated with the Metaverse. The predicted 2024 user penetration of essential Metaverse technologies (e.g., virtual world and blockchain asset use) is only 14.6% but is expected to reach 39.7% by 2030 (Statista, 2024b). This means that individuals who make up current statistics (e.g., empirical evidence on the effects of Metaverse-related technologies on behavior) have lived in an environment with little exposure to what would resemble the Metaverse. As a person's environment can influence their concept of morality (Piaget, 2013; Smetana and Jambon, 2017), the moral reasoning behind current individuals' behavior might not reflect that of individuals in our envisioned Metaverse world. For this reason, speculation and even divided opinions resulting from research (e.g., (Burkhardt and Lenhard, 2022; Coyne and Stockdale, 2021; Drummond et al., 2021; Ferguson et al., 2020; Malamuth, 2018) on the effects of violent media on violent behavior) could all be as relevant to the future—be seen as versions of the world. For instance, the less weight is placed on violence in the virtual, the more likely a person who has grown up in the Metaverse will suffer from identity confusion (section "Identity").

Cybercrimes. Cybercrimes are generally defined as acts committed through information and communication technologies that violate the law of the physical world (Charlton, 2024; Sukhai, 2004; United Nations Office on Drugs and Crime, 2019). We consider potentially major cybercrimes.

Virtual property crimes. In the virtual worlds and the Metaverse, individuals can create, own, modify, and exchange many virtual 'thing's, such as avatar accessory items, lands, artistic creations, cryptocurrencies (digital representations of value used for exchange through a decentralized digital ledger system, like blockchain (Huang et al., 2023)), other platform-specific exchange coins (e.g., Robux from Roblox (Roblox, 2023b)), etc. Similarly to their physical-world counterparts, these 'thing's can be damaged or stolen. For instance, people can vandalize virtual artworks with graffiti (BBC, 2017), causing permanent damage if their original data are overwritten with no backup (Seo et al., 2023). They can steal accessory items or platform currencies through scamming account information (BBC News, 2007) or hacking (Cavalli, 2008; JY Tan, 2024). While these 'thing's are virtual, many virtual worlds, like Roblox and Second Life, and cryptocurrency trading platforms (JY Tan, 2024) allow conversion with fiat currency, the medium of exchange (e.g., paper money or coins) (The Editors of Encyclopedia Britannica, 2024b) backed by a government that cannot be redeemed in gold or silver (The Editors of Encyclopedia Britannica, 2024c) (e.g., U.S. dollar, euro, or yuan). This can allow many to make a living by trading virtual 'thing's or services related to them (Brenner, 2008) (e.g., paid shifts in a virtual store in Roblox (Yandoli, 2024)).

A generally agreed upon criterion for taking legal actions against similar deprivation of a virtual 'thing' (e.g., Japan (Knight, 2005), the Netherlands (BBC News, 2007), and the United Kingdom (House of Commons Hansard, 2014)) is that the 'thing' needs to have 'real' monetary value (e.g., sold for "real cash" (Knight, 2005) or bought with "real money" (BBC News, 2007)). This could directly reflect an act's impact on the stability of the physical world's economic system (Seo et al., 2023). However, what qualifies as 'real' monetary value has been debated (Brenner, 2008; Wang, 2023). This led to cases where the deprivation of similar 'thing's (e.g., game accessories) was disregarded (BBC News, 2005; Cavalli, 2008).

To inform future debate, we illustrate how virtual 'thing's could be defined by law by considering the criteria that make a 'thing' a property—a 'thing' that can legally be owned but also has scarcity and value, in its use and/or its exchange (The Editors of Encyclopedia Britannica, 2024f). Scarcity implies that a 'thing' is limited in amount, not easily obtainable (Fairfield, 2022) in contrast to sunlight (Wang, 2023) or free, unlimited avatar accessories in existing game or Metaverse shops. Use value implies that the 'thing' can satisfy its owner's "subjective needs" (e.g., happiness), while exchange value is generally considered to be its value in fiat currency. While some believe that a property needs to have exchange value, others believe that use value is enough in many contexts (e.g., Japan and Germany), even when it is only for certain groups (e.g., game accessory by players and artwork by artists) (Wang, 2023). Given that some virtual artworks are currently worth millions of USD (JY Tan, 2024) and some virtual accessories and currencies, thousands (Cavalli, 2008), this broader definition could prevent their potential economic impact from being disregarded. To prevent identity confusion (section "Crimes"), the categorization of physical-world property (e.g., land, accessories, artworks, etc.) can serve as inspiration, but virtual 'thing's' unique characteristic in being easily duplicated through computational methods should be taken into consideration (Jiang, 2023; Wang, 2023).

While a physical-world object (e.g., one USD bill) cannot easily be increased in amount, in the virtual world, duplication could require only the changing of a single input value. This ease has

implications for the proportionality of punishment (section "Identity of AI and other computer-controlled entities"). To illustrate, in an existing case, a defendant took advantage of a game platform's system loophole to freely obtain game points worth 58,194 yuan (about 8135 USD) based on the trading pricing. While the court convicted the defendant for theft of such value, some consider the punishment disproportionate since the costs of distributing game points for the service provider are much less (Wang, 2023). In the Metaverse, treating a similar case based on the costs required to fix the hacking (Seo et al., 2023) or the trading price could affect recognition of a Metaverse economic system and thus integration of the virtual part of the Metaverse into the physical. As the more an individual is engaged with a virtual world, the more emotional value they give its virtual 'thing's (Strikwerda, 2012), making punishment for the deprivation of these 'thing's more severe could seem fairer to a growing amount of individuals with the growth of the virtual (section "Crimes"). It could also better reflect the loss of individuals who make their livings based on virtual 'thing's.

Money laundering through the Metaverse. Money laundering is a process by which criminals transform money of illicit origins (e.g., drug trafficking (Teichmann, 2020)) into money of seemingly legal ones (The Editors of Encyclopedia Britannica, 2024d). Money laundering in the Metaverse and in current platforms can be seen in three stages. The first is Placement, where illicit money is introduced into a (Metaverse) market in the form of virtual 'thing's (e.g., cryptocurrencies). The second is Layering, where the criminals obscure the origins of the money by creating a false proof through a series of transactions (e.g., purchasing through shell companies (Seo et al., 2023)). The third is Integration, where the money of now seemingly legal origins is put back into the main economic system (e.g., by being exchanged into fiat currency) (Mooij, 2024a). Cryptocurrencies, viable options for Metaverse currencies (section "Virtual property crimes"), have been used to facilitate money laundering because they are less detectable through anonymity during creation and the ease of splitting them into small amounts, require lower creation and transaction costs and can speed up the usually tedious Layering stage due to the lack of intermediary and geographical bounds (Mooij, 2024a; United Nations, 2024). Money laundering not only allows criminals to finance their activities but also propagates them. While the estimated amount of money laundered through cryptocurrencies fluctuates ($9.9 billion in 2020, $18.3 billion in 2021, $31.5 billion in 2022, and $22.2 billion in 2023), possibly due to new methods to evade detection (Chainalysis Team, 2024), the United Nations Office on Drugs and Crime estimates that money laundered each year amounts to 2% to 5% of the global GDP (800 billion to 2 trillion USD) (United Nations Office on Drugs and Crime, 2024)—which could reflect the use of cryptocurrency or another Metaverse coin. In fact, a study eliciting views on Metaverse crimes from experts (Gómez-Quintero et al., 2024) suggests that money laundering would be a "highly achievable" crime with "high harm".

The criminalization of money laundering, including through cryptocurrencies, is less contested, with many having taken legal actions (e.g., arrests or court cases from United Kingdom (Liz Jackson and PA Media, 2024), United States (Biase et al., 2024), Nigeria (Ogbonna, 2024), and China (Le, 2024), tax regulation helping victims by Algeria (Harff, 2024), and regulation to track transactions by Japan (Nikkei staff writers, 2022)). Though analyses of existing court cases, measures (Leuprecht et al., 2023; Mooij, 2024b; Thommandru and Chakka, 2023), and stakeholder opinions (Teichmann, 2020) suggest that the diversity of cryptocurrencies and regulatory measures could be a challenge for law enforcement efforts. This would require collaboration mainly with cryptocurrency market service providers and individuals (for private wallets) for investigation (e.g., the disclosure of transaction information (Reuters, 2022)) and standardization (e.g., standards for crime detection, such as requiring more personal information for a transaction at a standardized threshold (Mooij, 2024b)). Though this could challenge individuals' privacy rights and hopes for a decentralized Metaverse. We discuss solutions for information disclosure in the section "Possible approaches".

Tax violations in the Metaverse. Taxes are amounts of money that people are required to pay by a government mainly for its services, such as law enforcement efforts (Cox et al., 2024). Tax violations are crimes related to taxes, such as tax evasion (i.e., avoiding tax payment (Kagan, 2024)) and tax fraud (i.e., intentional disclosure of false information (Chen, 2024)). Not enforcing taxation in the Metaverse (e.g., for income earned in virtual worlds) could facilitate violations for taxes of the physical world, similarly to the cryptocurrency market (Kim, 2023), justifying the need for Metaverse taxes.

This raises questions on how the Metaverse should be taxed since existing tax laws are mainly based on one's relationship with different geographical jurisdictions (e.g., nationality, place of residence, or place of transaction). One way is for taxation to still be based on geographical jurisdictions. The main advantage is diminished costs in educating the public, already familiar with this concept. Though this would require physical-world identity information (e.g., IP address), which could easily be disguised (Kim, 2023). In fact, to combat tax evasion facilitated by anonymity, on March 2023, 48 countries agreed to follow transparency standards by exchanging information between each other and with cryptocurrency platforms (Singh, 2023). Though transparency could harm privacy, potentially discouraging participation in a Metaverse-like economy, as seen with a study on El Salvador (Alvarez et al., 2023), the first country to adopt a cryptocurrency as a currency. Moreover, taxation based on geographical jurisdictions could lead to the same type of transactions (e.g., in the same virtual world) being taxed differently across geographical jurisdictions. As inequity in amounts of taxes paid could lead to population migration (Kleven et al., 2020; Sandalci and Sandalci, 2021), this could destabilize the world with individuals with more sought-after skills becoming concentrated in specific areas. Taxation based on Metaverse jurisdictions (e.g., the virtual worlds; section "Rights and duties in Metaverse jurisdictions") could ensure greater equity and be easier to track (Kim, 2023) while ensuring greater privacy. As the Metaverse and its jurisdictions could have different government services (e.g., technical maintenance), taxes could be applied to both, similarly to federal (country) and territorial (jurisdictions within) taxes (e.g., (Canada Revenue Agency, 2024)).

Either way, international collaboration would be needed for information sharing and standardization, including agreement on the currency or the currencies recognized by the Metaverse's economic system. These could be fiat currencies, cryptocurrencies, or some new currencies. Despite the various opportunities for crimes that cryptocurrencies present, given their estimated market growth and their growing integration with our physical-world life (Statista, 2024a), ignoring them or banning them could be costly, not conductive to technological innovation, and even ineffective (Aquilina et al., 2024). Thus, the Metaverse would have to adopt existing cryptocurrencies or use some new currencies. If this Metaverse is decentralized, any new currencies could inherit cryptocurrencies' dangers, such as their volatility, their tendency to rapidly change in prices. Volatility is claimed to be behind many countries' reluctance in recognizing cryptocurrencies (e.g.,

China (BBC, 2021) and Qatar (The Peninsula Online, 2021)). From an accounting perspective, it leads to difficulties in assessing virtual 'thing's' value (e.g., for taxation purposes), which could lead to economic instability (Huang et al., 2023), large investment losses (Baur and Dimpfl, 2021; Yermack, 2024), and mistrust (Rehman et al., 2020). Trust impacted people's (lack of) acceptance of cryptocurrency as currency in El Salvador (Alvarez et al., 2023), potentially requiring more regulation (section "Ethical implications and other challenges during law enforcement").

Identity theft. Identity theft is a form of impersonation where the culprit uses the victim's personal information without their consent, possibly to commit fraud (Radin, 2024). Identity theft is a crime globally, with its protection service market expected to grow from 11.9 billion USD in 2024 to 28.1 billion USD in 2034 (Fact.MR, 2024). In the Metaverse, identity theft could occur with a culprit hacking into an individual's account then pretending to be them (e.g., through their avatar (Cheong, 2022)) or collecting identifying information (e.g., avatar appearance and gestures) then forging an avatar or a similar representation (Deng et al., 2023) to impersonate service providers (e.g., doctors) for payments (e.g., false medical advice), law enforcement officers for information crucial to the Metaverse's security (Gómez-Quintero et al., 2024), or someone's loved one to scam them for ransom from kidnapping without actually kidnapping the loved one (Geldenhuys, 2023; Sudhakar and Shanthi, 2023). Despite the existence of various measures for prevention (e.g., periodical changing of avatar appearance (Falchuk et al., 2018), authentication based on both biometrics and digital information (Yang et al., 2023), or splitting of personal information across the Internet network (Cheong, 2022)) and for detection (e.g., algorithms that analyze potentially AI-generated content's authenticity (Gupta et al., 2024)), they need to constantly evolve with technological advances and could be used to facilitate other crimes (Seo et al., 2023). As victims and perpetrators of the same cases can be across the world (Radin, 2024), international collaboration is needed for information sharing and technical standards (section "Ethical implications and other challenges during law enforcement").

Fantasy crimes. We explore major fantasy crimes.

Gambling. Gambling is the staking of a valuable 'thing' on the outcome of an uncertain event while knowing the risks and hoping to gain something out of it. Gambling games include poker, horse betting, slot machines, and lottery (Glimne, 2024). Gambling can be done in the physical world or online (e.g., virtual world's casino). Jurisdictions have varying levels of restrictions for (online) gambling, generally ranging from outright ban to allowing it under some age and game-type restrictions (The World Financial Review, 2022). Online gambling can impact individuals and society economically, through their physical-world finances and the ease of money laundering (Tomic, 2022), and psychologically, through the development of addiction (Brenner, 2008), aggravating negative economic impact in the long-term and a society's mental health (López-Torres et al., 2021). Gambling that does not involve 'real' money (e.g., the exchange of stakes with fiat currencies), 'simulated gambling" (Hing et al., 2022), has fewer legal restrictions, with even limited advice from the service provider (Hing et al., 2022). Though research has raised concerns, mainly about the transfer of simulated gambling habits to 'real' money gambling and other addictions (e.g., drugs), especially for younger individuals (Hing et al., 2022; Nower et al., 2022; Rahman et al., 2012). After a review of the research literature, the Albanese Government (Australia) decided to introduce age restrictions for simulated gambling starting from September 2024 (Ministers for the Department of Infrastructure, 2023). Similarly, the Consumer Council of Hong Kong has advocated for more legal restrictions in 2024 (Consumer Council, 2024). Similar to the case of media violence (section "Crimes"), the weight put on the harmful effects of simulated gambling versus individuals' freedom to explore could reshape society.

Prostitution. Prostitution is the practice of engaging in sexual activity to obtain immediate payment (Jenkins, 2024). While prostitution occurring in the physical world is more or less restricted legally (Nicola, 2021), prostitution occurring in the virtual is even more of a gray area. In existing virtual worlds (e.g., Second Life (Cavalli, 2009; Dane, 2020)) and similarly in the Metaverse, avatars can simulate sexual activity (Bellini, 2024) through animated visuals and wearable devices for touch sensation (Evans, 2023)) and obtain payment (Brenner, 2008) (e.g., in the platform's coins, which could be converted into fiat currency). When it does not involve a lack of consent (section "Virtual sexual assault"), a minor (i.e., someone not of consenting age), or someone looking like a minor (section "Sexual ageplay and child pornography"), the impact of this virtual prostitution could mainly be economical, as there are gains and losses of money, and psychological, due to embodiment (section "Identity").

To inform future decisions, we consider the pros and cons. Research on the physical world suggests that recognizing prostitution could be beneficial to society by making current underground prostitution transactions eligible for taxation (Al Hazmi, 2024), facilitating regulation of already existing prostitution-related crimes (e.g., human trafficking) (Lee and Persson, 2022), allowing marginalized groups to make a living (Yasin and Namoco, 2021), and decreasing rape rates and sexual violence (Gao and Petrova, 2022). The current existence of virtual prostitution suggests a demand for it, which could lead to a need to regulate similar consequent crimes (e.g., tax violations and trafficking of avatars (Gómez-Quintero et al., 2024)). Moreover, compared to its physical-world counterpart, virtual prostitution does not have health risks like sexually transmitted diseases or physical injury (Brenner, 2008). On the other hand, research in the physical world suggests that legalizing prostitution could influence the public's perception of the morality of "purchasing sex", potentially reshaping the world by expanding the market, leading to discriminatory behavior, and encouraging more criminal activities (e.g., sex trafficking) (Raymond, 2004). As virtual prostitution seems inevitable, a possible mediation is to contain it to specific areas both legally and computationally, requiring an understanding of different cultures, economies, and laws.

Virtual murder and physical assault leading to permanent damage to an avatar. Assault is an attempt at unlawfully using physical force against another (The Editors of Encyclopedia Britannica, 2024a). The digital version of acts harmful to humans physically cannot harm an avatar or any similar representation in the Metaverse unless it has been programmed (e.g., for violent video games) or hacked for this. When the original files are damaged, the harm done could warrant legal action (section "Virtual property crimes"). While the avatar is data that could 'belong' to one or several humans, it is also an extension of one's identity, psychologically and possibly legally (section "Identity"). Its categorization as a person who can have their own rights and duties or something else, such as property, could affect the victim's perception of fairness and others' recognition of the Metaverse identity. This could, in turn, encourage or discourage ethical

behavior (section "Crimes"). Across history, laws have treated the avatar's categorization differently, mainly between person and property (Andrade, 2009), leaning more toward non-person categories currently (Oleksii et al., 2024). Though many scholars advocate for a possibly new categorization: a legal person as allocating separate rights and duties could reduce ambiguities (Cheong, 2022), a balance between property and person, such as a property with stronger legal protection, to take into account its personal, emotional connection with the human behind (Andrade, 2009), or a balance between property and identity through a combination of existing categories (Oleksii et al., 2024). We discuss how the assessment of physical harm (which the definition of assault is grounded in) could be reflected through the assessment of psychological harm in the section "Virtual sexual assault".

Virtual sexual assault. Sexual assault is a form of assault involving some sexual conduct performed on a person without their consent (e.g., unwanted touching or sexual penetration) (Bellini, 2024). We consider sexual assault beyond the context of roleplay (i.e., consenting participants pretending). In the Metaverse, sexual assault could take the form of suggestive touching of the victim's avatar, sexual acts on their avatar (e.g., section "Introduction"), or the hacking of the platform to make avatars perform sexual acts on each other (Brenner, 2008; Dibbell, 2005). When there is no permanent destruction of data (section "Virtual murder and physical assault leading to permanent damage of an avatar"), the main impact of assault is psychological. As the definition of assault requires physical contact (The Editors of Encyclopedia Britannica, 2024a), criminalization of virtual sexual assault is still debated (Bellini, 2024; Gómez-Quintero et al., 2024).

The concept of embodiment (section "Identity") supports the similarity between psychological harm from acts in the virtual and that from the physical (as claimed in Camber (2024)'s case). For sexual acts specifically, research further supports the realism of sexual experiences through immersive technologies (Dekker et al., 2021), with the potential to reshape behaviors (Evans, 2023). The question is whether psychological harm can destabilize society enough to warrant legal action. Currently, the psychological impact of sexual assault (e.g., trauma) could lead to long-term effects, such as higher risks of engaging in other harmful behavior (e.g., hard drug use and contemplation of suicide), deteriorating relationships and work life, and a ripple effect with high costs to society (Bellini, 2024), with rape estimated to cost 122,461 USD across a victim's lifetime (Peterson et al., 2017). Based on potential harm severity, frequency, the ease of achieving it, and the ease of defeating it, experts have assessed virtual sexual assault as one of the top ten Metaverse crime risks (Gómez-Quintero et al., 2024). With advances in the realism of immersive technologies, both visual and multisensory, the impact of sexual assault on the victim could worsen. Not criminalizing virtual sexual assault could support already existing victim-blaming, stereotypes, and discrimination (Dyar et al., 2021; Stubbs-Richardson et al., 2018) and even affect sexual assault occurring in the physical world due to identity confusion (section "Crimes"). In terms of prevention specific to the Metaverse, specific user setting features (section "Ethical implications and other challenges during law enforcement") and restricted areas could be implemented (section "Prostitution") to balance different stakeholders' freedom. In line with legal tradition, the severity of punishment could be decided based on the psychological harm a "reasonable" person would suffer (Bellini, 2024), possibly with more recent population statistics. A similar line of reasoning could be applied to other acts where only psychological harm seems present (e.g., virtual physical assault outside the context of play).

Sexual ageplay and child pornography. Sexual ageplay legal in the physical world can be defined as consenting adults participating in sexual activity with one or several pretending to be a child or children. This is more controversial in the virtual since adults can make their avatars look different than what those of their chronological age usually look like. An example was Second Life, where some adult users engaged in sexual ageplay by donning avatars that look like children. Opinions among both users and the rest of the public (Brenner, 2008; Reeves, 2018) were divided. Proponents mainly argued that no 'real' child was hurt. Opponents mainly ranged from those who question the morality of sexual ageplay in general to those who question the visual depiction of children, 'real' or not, engaging in sexual acts. All worried about escalation to violence against 'real' children. This division is considered in line with the debate on virtual child pornography, entirely computer-generated sexually explicit graphics of "fictitious" children (Christensen et al., 2021). As both do not involve harm done to 'real' children, some lean toward protecting individuals' freedom. In *Ashcroft v. Free Speech Coalition* (Ward, 2009), the Court highlighted the absence of causality between consuming virtual child pornography and the harm that could follow (Ratner, 2021). While research does suggest that virtual child pornography could lead to addiction then crimes against 'real' children (Christensen et al., 2021), it also supports that a ban could lead to less tolerance even for what is legal (e.g., ban of child-looking avatars in general) (Reeves, 2018), potentially limiting more freedom than expected in the Metaverse. With advances in graphics and AI and the proliferation of cases of AI-generated pornography across the world (Bae and Yeung, 2023), international collaboration on the (non-)criminalization of virtual child pornography has become a pressing issue.

Simulation of the Holocaust and sensitive historical events. Prior work (Brenner, 2008, pp. 95–96) mentions the hypothetical situation of the reconstruction of a Nazi death camp where users can roleplay as Nazis and inmates. While this would be illegal in many European countries, it would not be in the United States. An analysis (Cowan and Maitles, 2011) of simulations of sensitive historical events (e.g., Holocaust) and scenarios (e.g., racism) reveals opinions as divided—even when they were intended to increase empathy. Cons include perceived disrespect toward the victims due to lack of accuracy (Cowan and Maitles, 2011), identity confusion if such acts are popularized (section "Crimes"), and other potential impact on the mental health of those role-playing and the audience, such as increased fear of future terrorism due to graphic media (Holman et al., 2020). A possible mediation with one's freedom could be to raise awareness about potential harms but still allow simulations (e.g., for artistic expression and education) with stricter conditions (e.g., not in publicly accessible areas), requiring cultural and historical insights from different jurisdictions.

Law enforcement

An international legal framework for the Metaverse would not be the first attempt at establishing a commonly agreed upon legal framework among jurisdictions. A close example is that of cyberspace. One main source of challenges, which has prevented the establishment of an international legal framework for cyberspace (Gajjar and Taherdoost, 2024), is the difficulty in resolving differing views among stakeholders (Weber, 2015). Referring to prior work, we provide insights on stakes to consider for governance in the Metaverse (section "Governance") and possible approaches to challenges across the law enforcement process (section "Ethical implications and other challenges during law enforcement"), including ethical implications.

Governance

A balance. While many hope for the Metaverse to be unrestricted by geographical jurisdictions and have decentralized governance, a historical examination of cyberspace (Weber, 2015) suggests that the long-term survival of a similar space connecting the virtual and the physical depends on a balance of the influence of three stakeholder groups—geographical jurisdiction governments, service providers, and individuals—and a balance between centralized and decentralized governance.

Each stakeholder group can influence the existence of the Metaverse: service providers provide essential technologies (Wu and Zhang, 2023), individuals finance the Metaverse, and governments provide law enforcement resources and establish laws in the physical world (INTERPOL, 2024a; Seo et al., 2023), where individuals and service providers are based. However, leaning toward one group could result in fragmentation, the splitting of the Metaverse (Gajjar and Taherdoost, 2024), and instability of the physical world. As seen in *Snow Crash*, more power for service providers could lead to the splitting of geographical jurisdictions by them (Stephenson, 2022), possibly resulting in the loss of individuals' rights. Too much government regulation could harm technological innovation (Wiener, 2004) and shift the power to a few more powerful countries. Leaving the rule entirely to individuals could lead to the power shifting to a few—service providers with more popular platforms or technologies, more powerful governments, or 'wealthier' individuals—who might not always represent the majority's views (Goldberg and Schär, 2023; Weber, 2015).

Though balancing the influence of stakeholder groups on decision-making would depend on how centralized or decentralized governance is. An example of decentralized governance is where each stakeholder can cast a vote that directly counts toward decision-making. An extreme example of centralized governance could be where a single authority, made of a few individuals, makes decisions for the entire Metaverse without consulting the other stakeholders. A mediation could be where a central authority made of elected representatives participates in final decision-making processes (Aristotle, 1885). Despite arguments against centralized governance (Chao et al., 2022; Goldberg and Schär, 2023; Karaarslan and Yazici Yilmaz, 2023), history suggests that leaning toward the extremes of either centralization or decentralization might lead to the loss of qualities essential to the existence of an international legal framework. A legal framework's existence can be seen as a result of reliability (trust in its fairness by those ruled) and practicality (balance between costs of enforcing the laws versus not enforcing) (Bellini, 2024). Though fairness is a subjective assessment influenced by perceptions of the legal framework's adaptability (e.g., to socio-cultural nuances, technological advances, and case-specific details (Gómez-Quintero et al., 2024)) and consistency, how standardized the law enforcement process is (e.g., for punishment and compensation for a specific group) (Weber, 2015).

For a specific case, leaning toward decentralized governance by including opinions of not only representatives but also of specific witnesses could provide insights on socio-cultural nuances, which could improve adaptability. For instance, consider two cases of virtual sexual ageplay: the first occurs in a virtual world specifically designed for adult individuals wanting to engage in this type of play, while the second occurs in a virtual world that is for the general public. Members of the two different virtual worlds might have different views on the impact of sexual ageplay on their specific worlds, with those of the first possibly being more accepting (section "Sexual ageplay and child pornography"). This nuance could lead to different assessments of the harm done by similar acts, affecting perceptions of fairness for specific decisions. Though too much adaptability could also harm perceptions of fairness with less consistency, leading to loopholes and a lack of incentives. A parallel can be drawn with an analysis of attempts at ensuring child safety in cyberspace (Rahamthaulla, 2020), which suggests that a greater authority, a government, overseeing platforms' regulation might be more suitable than leaving regulation entirely to platforms as they would lack the financial incentives to enforce rules. Decentralization with no central authority could also lead to a lack of standardization, making law enforcement seem less transparent and complicate collaboration due to differing views (INTERPOL, 2024a). Thus, a certain degree of centralization might be necessary for reliability (Weber, 2015).

Practicality also requires a balance between decentralization and centralization. 'Decentralized' law enforcement efforts among governments and service providers could diminish costs when collecting or analyzing evidence due to varying familiarity with territories and technologies. Though no central authority to ensure collaboration could increase costs due to conflicts (section "Ethical implications and other challenges during law enforcement"). Moreover, without technical standards (e.g., user devices and data formats), law enforcement would require costly additional resources (e.g., to extract information from different devices) (Seo et al., 2023).

Governance through technologies. As the Metaverse depends on computational technologies, governance is limited by their capabilities (Zwitter and Hazenberg, 2021). As existing technologies facilitating decentralized governance come with limitations, a balance between centralization and decentralization might be the most technically realistic option.

From a high level, less centralization can improve the security of the Metaverse but hinder law enforcement. The Metaverse can be seen as a network of nodes, units that can receive, store, process, and send information that is more or less crucial to the Metaverse's functioning (e.g., authentication information from the user's device to a virtual world platform or evidence between law enforcers' servers). In a centralized network, all information passes through a single node or a small number of closely connected nodes. Thus, if a single node or a small number is attacked or malfunctions, the entire Metaverse would stop functioning. For a less centralized network, information can pass through several not closely connected nodes. Thus, even if a few are attacked or malfunctioned, the Metaverse would still be functioning partially (Karaarslan and Yazici Yilmaz, 2023). Similarly, if a central authority requires that all information be processed by its own server, it faces the security risks of a centralized network. Though avoiding such risks through several servers spread out across the Metaverse could complicate the law enforcement process (section "A balance") due to the scale and the diversity of data formats (Seo et al., 2023).

Among specific technologies, blockchain and AI could facilitate decentralized governance. Blockchain is a digital ledger system for monitoring and recording transactions (e.g., votes) without any intermediary (Wang et al., 2022). In other words, any authenticated individual could directly influence a specific decision by registering their vote by themself. An example is Decentraland, the first large-scale virtual world that uses blockchain, and a Decentralized Autonomous Organization (DAO), the decentralized collective that governs through blockchain. There, an individual can vote for a decision by signing a message with Identification information (section "Identity"). This message will then be publicly accessible in the blockchain to ensure transparency and tracking of voting results. Once the voting period ends, votes are summed up, then the decision is executed by a committee made of members elected through a similar decentralized fashion (Goldberg and Schär,

2023). Though blockchain might not be sufficient for entirely decentralized governance in terms of both practicality and reliability.

In terms of practicality, given the scale of the Metaverse, the scalability of blockchain, and its adaptability to a large network, could come at the cost of decentralization (Wang et al., 2022; Xie et al., 2019). For a single blockchain system, the more there are nodes in the network (e.g., individual voters' devices), the slower activities in the Metaverse will become (Karaarslan and Yazici Yilmaz, 2023). Splitting the blockchain into several could improve scalability and security (e.g., difficulty in stealing information due to data format differences) but lead to loopholes, such as fraud, where the same individual uses different accounts in different blockchains to vote for the same decision (Wu and Zhang, 2023), and unreliable votes, where an individual who has lost their voting right for one blockchain from misbehavior might still be seen as an upstanding voter in another due to separate criminal records (Banaeian Far and Hosseini Bamakan, 2023). A possible solution is to associate each individual with the same set of Identification information. Though, depending on the information used (e.g., government-issued IDs or biometrics detected by specific service providers' devices), governments or service providers' influence could break the balance of stakes (section "A balance"). Moreover, if service providers have full control over their blockchains (e.g., by being their creators) with no central authority overseeing Metaverse governance, they could collude with each other, compiling user profiles based on their unique identifiers (Banaeian Far and Hosseini Bamakan, 2023). A neutral central authority establishing standards and managing Identification information could mitigate aforementioned issues.

A main challenge to fairness (reliability) in blockchain-based governance is the difficulty to reach a decision that balances the stakes of all stakeholders. Giving the same weight to each vote might not be seen as fair, reflect the impact on different stakeholders who might have different amounts of investment (Goldberg and Schär, 2023), and increase vulnerability to fraud (Scharfman, 2024). For this reason, most DAOs employ token-based voting, where each user's vote is weighted based on the amount of assets they own (e.g., virtual land parcels). Proponents argue that this ensures fairness by allowing those with the most exposure to the world to decide about it. Though the analysis of 1414 governance proposals in Decentraland (Goldberg and Schär, 2023), which has adopted such token-based voting, suggests that dominant voters' choices do not always reflect the consensus among other voters, highlighting the difficulty in ensuring fairness to the majority and the greater good. Instead of leaving power allocation to a more natural course of events, a central authority made of not only elected representatives but also domain experts (Weber, 2015) (e.g., law, computer science, and cultural studies) could lead to decisions more beneficial to the general public.

Many have envisioned AI as support for decentralized governance that improves practicality and reliability. AI technologies could improve time efficiency and security by automating different processes, such as the analysis of large quantities of votes or law enforcement evidence and the automatic detection of suspicious activities (Hakan Kan, 2024; He et al., 2021; Li et al., 2016). Though, while they have been envisioned to improve fairness by reducing the biases humans make during decision-making, AI technologies come with biases of their own (e.g., against ethnic groups) (Charles et al., 2022; Henman, 2020; Ntoutsi et al., 2020), which could lead to wrong decisions during law enforcement (Seo et al., 2023). Empirical evidence suggests that humans and AI could have complementary roles during decision-making. For instance, humans can be more adaptable to specific contexts, and AI, is more adaptable to the general public's preferences (Papagiannidis et al., 2023). Collaboration between humans and AI could thus surpass the performance of humans or AI alone (Inkpen et al., 2023; Ren et al., 2023). For best performance, governance with AI would need some humans, but to ensure neutrality, these humans would need to either belong to some central neutral authority or follow AI usage standards overseen by it (Ferrari et al., 2023), requiring a balance between centralization and decentralization.

Rights and duties in Metaverse jurisdictions. In the physical world, the assignment of legal rights and duties is mainly based on a person's identity attributes (section "Identity") relevant to their relationship with the geographical jurisdiction they are in and the one(s) they belong to (nationality). A transition to the Metaverse, a space unbounded by geography, will require a novel view. To balance centralization and decentralization (section "Governance"), a solution, supported by physical-world (Aristotle, 1885; Blaustein, 2015), cyberspace (Rahamthaulla, 2020; Schneider et al., 2021; Weber, 2015), and Metaverse (Fernandez and Hui, 2022; Yang, 2023b) works, is a form of bottom-up governance, where a person would have rights and duties from a Metaverse level but also for individual modules (i.e., virtual worlds and other communities that might be larger or smaller), Metaverse jurisdictions, which independently regulate less severe violations. We discuss in detail identity attributes that could be used to ensure the quality of votes: citizenship, chronological age, and criminal record.

In the physical world, citizenship is considered the form of nationality with the most privileges (The Editors of Encyclopedia Britannica, 2023), including voting rights. Application for citizenship requires proof of potential commitment toward the greater good of the jurisdiction, which can include a required period of residence, intention to reside in the jurisdiction, one's age, and their criminal record (The Editors of Encyclopedia Britannica, 2024e). Similarly, citizenship could be equivalent to the most privileged form of membership in the Metaverse or module, requiring a certain amount of time spent in the Metaverse or module, involvement (e.g., investment in assets as seen with Decentraland (Goldberg and Schär, 2023)), one's age, and their criminal record.

In the physical world, the minimum voting age varies across geographical jurisdictions, with debate on whether an individual at a specific age has the appropriate decision-making competence (e.g., cognitive development and experience in politics) to represent the people's needs. Some also question the use of age as a criterion, proposing that success in a test on decision-making capabilities (Wagner et al., 2012), such as literacy and the ability to make independent choices, could be used instead (Cook, 2013). While such a method could improve reliability, it could harm practicality, at least in the near future, as additional resources would be needed to administer the test and educate the public. In the Metaverse, there could be a Metaverse-level minimum voting age or equivalent criterion. As age is also a criterion for access to mature content (Brenner, 2008; Rahamthaulla, 2020), a module could set additional restrictions on age or an equivalent. A challenge is deciding whether a module can have fewer restrictions on voting. Since a module could represent a community mainly made of users younger than the voting age, as seen with Roblox (Clement, 2024; Eichhorn and Bergh, 2021), requiring a higher age could lead to a small group of individuals making decisions not representative of the majority's opinions. As a factor for determining the voting age is familiarity with the jurisdiction's politics (Wagner et al., 2012), a possible solution is to assign module-level voting rights based on familiarity with the module along with basic reading comprehension capabilities. Another solution is to give the voting right to an eligible guardian (e.g., parent), similar to the physical world (Cook, 2013).

Misbehavior could also occur during voting in the Metaverse. This could be automatically detected (section "Governance through technologies") or reported by users. Reputation scores associated with the individual's identity could then be computed (Fernandez and Hui, 2022) and made accessible across modules to prevent loopholes (section "Governance through technologies").

Ethical implications and other challenges during law enforcement. Law enforcement is generally seen as fulfilling the following purposes: prevention, detection, investigation, and prosecution (Bellini, 2024; Reingnaum, 1993; Seo et al., 2023) of a potential crime. In the Metaverse, prevention includes educating the public (e.g., raising awareness about the dangers of identity confusion in sections "Identity" and "Crimes"), developing governance measures (e.g., blockchain-based architecture to prevent collusion and disclosure of criminal records to diminish risks of fraud during voting), and implementing preventive platform features for users (e.g., a bubble around an avatar to keep others distanced, potentially preventing crimes involving the physical contact of virtual bodies (Bellini, 2024)). Detection includes the report of misbehavior and its surveillance through computational methods by collecting and then processing information from the different layers of identity. For instance, by analyzing information from the Identification and Data layers, algorithms could detect fraud during voting (sections "Identity" and "Governance through technologies"). By analyzing Representation information, they could detect offensive speech (Babaeianjelodar et al., 2022) or closeness between virtual bodies (Wang et al., 2024a), which can suggest potential crimes, such as virtual sexual assault (Bellini, 2024). Investigation includes finding where the evidence is (e.g., the device and the virtual and/or physical world(s)), identifying the formats of the evidence, securely retrieving the evidence (e.g., by encrypting it), synthesizing the evidence (possibly with the help of AI), and drawing conclusions (Seo et al., 2023). Prosecution is the act of holding a trial against a person to see whether they are guilty of a crime (Merriam-Webster, 2024c). Detection, investigation, and prosecution can also intersect with prevention. The knowledge that one's misbehavior can be detected as evidence to prove their guilt and exposed to the public can deter crimes (Gómez et al., 2021) through lower perceived success rates (Gómez-Quintero et al., 2024) and greater awareness of the consequences, such as shame (Johnson, 2020). The mere awareness of being watched can also encourage individuals to report crimes (Shore et al., 2022).

Stakes and challenges. For each purpose of law enforcement, the stakes of main stakeholder groups could be affected, risking balance in the Metaverse (section "A balance").

While identifying information can support law enforcement (section "Ethical implications and other challenges during law enforcement"), individuals' awareness that they have less privacy, freedom of keeping sensitive identity information from others (Merriam-Webster, 2024b), could affect their motivation to join the Metaverse (section "Ethical implications and other challenges during law enforcement"). As perceived immoral behaviors that might not be criminalized (e.g., offensive comments) could lead to public aggression targeted at the culprit (e.g., offensive comments and unauthorized exposure of private information), leading to consequences beyond punishment prosecution would be deemed suitable (Fritz, 2021), making criminal records publicly accessible can be morally questionable (Billingham and Parr, 2020; Blitvich, 2022) and impact society's stability. While laws could limit information access to authorized parties only, as is currently done (e.g., European Union (Wolford, 2024), China (Law, 2022), and Switzerland (Confederation, 2023)), perceptions about the security of one's information (e.g., from theft (Wu and Zhang, 2023) or unauthorized monetization (Chen et al., 2022)) could negatively affect willingness to disclose information (Heirman et al., 2013; Mutimukwe et al., 2020).

As data is mainly collected through service providers' devices and platforms, their cooperation can diminish costs but could harm their profits (e.g., costs in assisting law enforcement or implementing technical standards) and their clients' stakes. In fact, on the grounds of user privacy, service providers could refuse to cooperate, as seen with prior terrorism investigation (Seo et al., 2023).

Collaboration with governments is necessary as law enforcement might involve evidence from their geographical jurisdictions, such as data about them (e.g., camera footage from devices (Lee et al., 2021)) or from servers physically located in them (INTERPOL, 2024a). Though collaboration could diminish a government's sovereignty, its authority over matters within its territory and related to its nationals. As many jurisdictions' laws ensure their control over not only resources physically within their territories but also those associated with their nationals outside, laws can spill over each other, leading to conflict when sharing resources (Weber, 2015). For instance, as online service providers (e.g., Microsoft and Amazon) are physically stationed all over the world, a jurisdiction and its nationals can have data stored in the territory of a different jurisdiction, which could lead to confusion about which jurisdiction's laws to follow and whose law enforcement officers should handle the data (Kushwaha et al., 2020). The Metaverse could inherit similar issues among geographical jurisdictions but also among modules (service providers behind).

Possible approaches. We provide insights for solving issues mentioned in the section "Stakes and challenges" based on existing works and attempts.

To encourage information disclosure, several approaches can be considered separately or together. In compliance with existing laws on data privacy (e.g., (Wolford, 2024)), the Metaverse can support the disclosure of minimal identity information (e.g., for citizenship application or for investigation). Research has shown the technical viability of selectively disclosing information for a blockchain-based system (Mukta et al., 2020). From a legal perspective, we can protect an individual's physical-world identity by extending upon arguments of prosecuting avatars like organizations recognized as legal persons (Cheong, 2022), which can allow anonymity of the humans. As an avatar may not be a necessary component of Metaverse identity (Gómez-Quintero et al., 2024), the avatar(s) could be part(s) of the Metaverse identity that defines the legal person. Moreover, the Metaverse could encourage information disclosure by giving individuals more control (Benson et al., 2015), by allowing them to join with less sensitive information and by enabling features as they provide more information. This is done by many existing platforms. For instance, Roblox (Roblox, 2023b) does not require any government-issued physical-world identifier for account creation, but using such an identifier to verify one's age can give them access to more mature content (Roblox, 2023a). Similarly, in the Metaverse, disclosing or verifying one's age can be optional for account creation but required for mature content and voting rights. Other measures include raising awareness about the security of the Metaverse and describing the use of data (e.g., privacy policy) during account creation (Zhang et al., 2020).

For collaboration among jurisdictions (geographical or modules), while variation among laws and rules could lead to many challenges (section "Stakes and challenges"), it could also improve adaptability and practicality (section "A balance"). A neutral

central authority with elected representatives might thus need to oversee law enforcement efforts to a certain extent. Similarly to INTERPOL, such an authority could mainly coordinate law enforcement efforts belonging to existing jurisdictions (Gilsinan, 2014; INTERPOL, 2024b). We consider 4 non-discrete levels of control over the law enforcement process to illustrate possible approaches for future reference. For the first level, the authority can have its own data storage system and law enforcement officers who can obtain warrants to search physical locations in geographical jurisdictions and arrest individuals. While this could avoid many conflicts between laws and rules, this might not be feasible due to computing costs (Seo et al., 2023), security risks (section "Governance through technologies"), and the compromises service providers and governments have to make (section "Stakes and challenges"). In the second level, the authority acts more as a coordinator, ensuring communication between the law enforcement efforts of all stakeholders concerned (e.g., representative of the jurisdiction a suspect belongs to, representative of a different jurisdiction in which the suspect's data is stored, and representatives of related service providers). Only in case of conflicts does the authority send in its own personnel. In the third level, the authority acts as a coordinator with no such personnel, with conflicts being resolved through discussion with all stakeholders. In the fourth level, the authority does not participate in any decision, with only stakeholders voting in case of a conflict and the authority ensuring the execution of the decision. This is similar to Decentraland (section "Governance through technologies") and thus could inherit its difficulty in weighting votes.

Conclusion

Diversity among stakeholders in the Metaverse across time and place requires an international legal framework that continuously balances stakes across technological and socio-cultural changes. Given that the Metaverse has yet to exist, we combine speculation with both theory and empirical evidence (section "Introduction") to present insights that could inform legal decisions related to identity (section "Identity"), crimes (section "Crimes"), and law enforcement (section "Law enforcement"). We also suggest possible future research directions to further bridge the gap between the present and the future (section "Future research directions").

Future research directions. Future research could seek to better understand law enforcement from the user's perspective. Through scenarios explored in our work, future research could obtain user's preferences for privacy measures (section "Ethical implications and other challenges during law enforcement"), for punishment and compensation of specific acts (section "Crimes") in specific virtual worlds for socio-cultural nuances (section "A balance"), and for voting criteria (section "Rights and duties in Metaverse jurisdictions"). Future research could also obtain feedback from experts in psychology, education, and technology, respectively, for detecting emotional harm (section "Crimes"), raising awareness about legal concerns (section "Ethical implications and other challenges during law enforcement"), and finding suitable technical standards (e.g., for AI in section "Identity of AI and other computer-controlled entities" and data formats in section "Law enforcement"). Longitudinal studies could explore the effects of immersive technology use on cognitive development for different age groups and the efficiency of different technologies, such as blockchain, on supporting governance outside the experimental setting, possibly by looking at existing virtual worlds (e.g., (Karaarslan and Yazici Yilmaz, 2023)).

Data availability

Data sharing is not applicable to this article as no datasets were generated or analyzed during the current study.

Received: 31 December 2023; Accepted: 13 December 2024;
Published online: 12 February 2025

References

Abbott R, Sarch A (2024) Punishing artificial intelligence: legal fiction or science fiction. In: Moura Vicente D, Soares Pereira R, Alves Leal A (eds.) Legal aspects of autonomous systems. Springer International Publishing, Cham. pp. 83–115
Al Hazmi RA (2024) Underground economy and taxation of prostitution (literature study in indonesia). Educoretax 4(3):388–394
Al Tamimi Y (2018) Human rights and the excess of identity: a legal and theoretical inquiry into the notion of identity in strasbourg case law. Soc Leg Stud 27(3):283–298
Ali W, Tian W, Din SU, Iradukunda D, Khan AA (2021) Classical and modern face recognition approaches: a complete review. Multimed Tools Appl 80(3):4825–4880
Alvarez F, Argente D, Patten DV (2023) Are cryptocurrencies currencies? Bitcoin as legal tender in el salvador. Science 382(6677):eadd2844
Andrade NNGD (2009) Striking a balance between property and personality: the case of the avatars. J Virtual Worlds Res 1(3):53
Aquilina M, Frost J, Schrimpf A (2024) Tackling the risks in crypto: choosing among bans, containment and regulation. J Jpn Int Econ 71:101286
Aristotle (1885) The Politics. Clarendon Press
Asimov I (2004) I, Robot. Robot. Spectra Books
Babaeianjelodar M, Poorna Prudhvi G, Lorenz S, Chen K, Mondal S, Dey S et al. (2022) Interpretable and high-performance hate and offensive speech detection. In: Chen JYC, Fragomeni G, Degen H, Ntoa S (eds.) HCI International 2022—Late Breaking Papers: Interacting with eXtended Reality and Artificial Intelligence. Springer Nature Switzerland, Cham. pp. 233–244
Bae G, Yeung J (2023) South Korea has jailed a man for using ai to create sexual images of children in a first for country's courts. CNN
Balaban RB (2000) A physician's guide to talking about end-of-life care. J Gen Intern Med 15(3):195–200
Banaeian Far S, Hosseini Bamakan SM (2023) Nft-based identity management in metaverses: challenges and opportunities. SN Appl Sci 5(10):260
Barbosa MM (2024) Autonomous systems and tort law. In: Moura Vicente D, Soares Pereira R, Alves Leal A (eds.) Legal aspects of autonomous systems. Springer International Publishing, Cham, pp. 3–23
Baur DG, Dimpfl T (2021) The volatility of bitcoin and its role as a medium of exchange and a store of value. Empir Econ 61(5):2663–2683
BBC (2017) BBC Artist 'vandalises' Snapchat's AR Balloon Dog sculpture. BBC
BBC (2021) BBC China declares all crypto-currency transactions illegal. BBC
BBC (2024) BBC Google to fix AI picture bot after 'woke' criticism. BBC
BBC (2005) BBC News 'Game theft' led to fatal attack. BBC
BBC (2007) BBC News 'Virtual theft' leads to arrest. BBC
Bellini O (2024) Virtual justice: criminalizing avatar sexual assault in metaverse spaces. Mitchell Hamline Law Rev 50(1):3
Benson V, Saridakis G, Tennakoon H (2015) Information disclosure of social media users. Inf Technol People 28(3):426–441
Biase N, Scarff L, Wratchford S (2024) Founders and CEO of cryptocurrency mixing service arrested and charged with money laundering and unlicensed money transmitting offenses. United States Attorney's Office Southern District of New York
Billingham P, Parr T (2020) Enforcing social norms: The morality of public shaming. Eur J Philos 28(4):997–1016
Blaustein J (2015) Community policing from the 'bottom-up'. In: Speaking truths to power: policy ethnography and police reform in Bosnia and Herzegovina. Oxford University Press
Blitvich PG-C (2022) Moral emotions, good moral panics, social regulation, and online public shaming. Lang Commun 84:61–75
Bond P (2022) Eu, South Korea, Japan announce metaverse regulation plans. Holland & Knight
Brenner SW (2008) Fantasy crime: the role of criminal law in virtual worlds. Vand J Ent Tech L 11:1
Bryson JJ, Diamantis ME, Grant TD (2017) Of, for, and by the people: the legal lacuna of synthetic persons. Artif Intell Law 25(3):273–291
Burkhardt J, Lenhard W (2022) A meta-analysis on the longitudinal, age-dependent effects of violent video games on aggression. Media Psychol 25(3):499–512
Burrows M, Abadi M, Needham R (1990) A logic of authentication. ACM Trans Comput Syst 8(1):18–36

Camber R (2024) British police probe VIRTUAL rape in metaverse: young girl's digital persona 'is sexually attacked by gang of adult men in immersive video game'—sparking first investigation of its kind and questions about extent current laws apply in online world. Daily Mail Online
Canada Revenue Agency (2024) Provincial and territorial tax and credits for individuals. Government of Canada. https://www.canada.ca/en/revenue-agency/services/tax/individuals/topics/about-your-tax-return/tax-return/completing-atax-return/provincial-territorial-tax-credits-individuals.html. Accessed 14 Aug 2024
Casado EM (2024) Robots and liability: new criteria and attribution methods. In: Moura Vicente D, Soares Pereira R, Alves Leal A, (eds.) Legal aspects of autonomous systems. Springer International Publishing, Cham. pp. 117–137
Cavalli E (2008) Police refuse to aid in virtual theft case. Wired
Cavalli E (2009) Italian woman explores prostitution via second life. Wired
Chainalysis Team (2024) Money laundering activity spread across more service deposit addresses in 2023, plus new tactics from lazarus group. Chainalysis
Chao C-H, Ting I-H, Tseng Y-J, Wang B-W, Wang S-H, Wang Y-Q et al. (2022) The study of Decentralized Autonomous Organization (DAO) in social network. In: Proceedings of the 9th Multidisciplinary International Social Networks Conference, MISNC '22. Association for Computing Machinery, New York, NY, USA. pp. 59–65
Charles V, Rana NP, Carter L (2022) Artificial intelligence for data-driven decision-making and governance in public affairs. Gov Inf Q 39(4):101742
Charlton E (2024) was a big year for cybercrime—here's how we can make our systems safer. World Economic Forum
Chen J (2024) What is tax fraud? Definition, criteria, vs. tax avoidance. Investopedia
Chen Z, Wu J, Gan W, Qi Z (2022) Metaverse security and privacy: an overview. In: 2022 IEEE International Conference on Big Data (Big Data), pp. 2950–2959
Cheong BC (2022) Avatars in the metaverse: potential legal issues and remedies. Int Cybersecur Law Rev 3:1–28
Christensen LS, Moritz D, Pearson A (2021) Psychological perspectives of virtual child sexual abuse material. Sexuality Cult 25(4):1353–1365
Clement J (2024) Distribution of Roblox audiences worldwide as of December 2023, by age group. Statista
Collard AM (2022) Crime in the metaverse is very real. But how do we police a world with no borders or bodies? World Economic Forum
Confederation S (2023) Federal act on data protection. Fedlex
Consumer Council (2024) Simulated gambling games full of tactics to lure in-game purchases tougher regulation urged to steer players away from addiction. Consumer Council
Cook P (2013) Against a minimum voting age. Crit Rev Int Soc Political Philos 16(3):439–458
Cowan P, Maitles H (2011) Teaching the holocaust: to simulate or not? Race Equal Teach 29(3):46–47
Cox MS, Neumark F, McLure CE (2024) Taxation. Britannica Money
Coyne SM, Stockdale L (2021) Growing up with grand theft auto: a 10-year study of longitudinal growth of violent video game play in adolescents. Cyberpsychol Behav Soc Netw 24(1):11–16
Danaher J (2016) Robots, law and the retribution gap. Ethics Inf Technol 18(4):299–309
Dane K (2020) Second life for prostitution: a blogger spoke about the work of a virtual brothel in second life. FreeMMORPG.top
Dekker A, Wenzlaff F, Biedermann SV, Briken P, Fuss J (2021) Vr porn as ëmpathy machine?¨ perception of self and others in virtual reality pornography. J Sex Res 58(3):273–278
Deng M, Zhai H, Yang K (2023) Social engineering in metaverse environment. In: 2023 IEEE 10th International Conference on Cyber Security and Cloud Computing (CSCloud)/2023 IEEE 9th International Conference on Edge Computing and Scalable Cloud (EdgeCom). pp. 150–154
Dibbell J (2005) A rape in cyberspace. Village Voice
Dobrygowski D, Espinoza J, Li C, Reim D, Price M, Schilling A et al. (2024) Metaverse identity: Defining the self in a blended reality. Technical report. World Economic Forum
Doomen J (2023) The artificial intelligence entity as a legal person. Inf Commun Technol Law 32(3):277–287
Drummond A, Sauer JD, Ferguson CJ, Cannon PR, Hall LC (2021) Violent and non-violent virtual reality video games: Influences on affect, aggressive cognition, and aggressive behavior. two pre-registered experiments. J Exp Soc Psychol 95:104119
Dyar C, Feinstein BA, Anderson RE (2021) An experimental investigation of victim blaming in sexual assault: the roles of victim sexual orientation, coercion type, and stereotypes about bisexual women. J Interpers Violence 36(21-22):10793–10816
Eichhorn J, Bergh J (2021) Lowering the voting age to 16 in practice: Processes and outcomes compared. Parliamentary Aff 74(3):507–521
El Naqa I, Murphy MJ (2015) What is machine learning? Springer International Publishing, Cham, p 3–11
European Parliament (2024) EU AI act: first regulation on artificial intelligence. European Parliament
Evans L (2023) Virtual reality pornography: a review of Health-Related opportunities and challenges. Curr Sex Health Rep 15(1):26–35
Fact.MR (2024) Identity theft protection services market (2024 to 2024). Fact.MR
Fairfield J (2022) Property as the law of virtual things. Front Res Metr Anal 7:981964
Falchuk B, Loeb S, Neff R (2018) The social metaverse: Battle for privacy. IEEE Technol Soc Mag 37(2):52–61
Feng C (2024) China convenes Huawei, Tencent, Baidu to draft metaverse standards in bid to become global technology leader. South China Morning Post
Ferguson CJ, Copenhaver A, Markey P (2020) Reexamining the findings of the American psychological association's 2015 task force on violent media: a meta-analysis. Perspect Psychol Sci 15(6):1423–1443
Fernandez CB, Hui P (2022) Life, the metaverse and everything: An overview of privacy, ethics, and governance in metaverse. In: 2022 IEEE 42nd International Conference on Distributed Computing Systems Workshops (ICDCSW). IEEE. pp. 272–277
Ferrari F, van Dijck J, van den Bosch A (2023) Observe, inspect, modify: three conditions for generative ai governance. N Media Soc 0(0):14614448231214811
Feuerriegel S, Hartmann J, Janiesch C, Zschech P (2024) Generative AI. Bus Inf Syst Eng 66(1):111–126
Fritz J (2021) Online shaming and the ethics of public disapproval. J Appl Philos 38(4):686–701
Gajjar VR, Taherdoost H (2024) Cybercrime on a global scale: trends, policies, and cybersecurity strategies. In: 2024 5th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI). IEEE, pp. 668–676
Gao H, Petrova V (2022) Do prostitution laws affect rape rates? Evidence from Europe. J Law Econ 65(4):753–789
Geldenhuys K (2023) Virtual kidnapping. Servamus Community-based Saf Security Mag 116(11):34–36
Genay A, Lécuyer A, Hachet M (2022) Being an avatar "for real": a survey on virtual embodiment in augmented reality. IEEE Trans Vis Comput Graph 28(12):5071–5090
Gilsinan K (2014) Interpol at 100: does the world's police force work? The Atlantic
Glimne D (2024) Gambling. Britannica
Gómez-Quintero J, Johnson SD, Borrion H, Lundrigan S (2024) A scoping study of crime facilitated by the metaverse. Futures 157:103338
Goldberg M, Schär F (2023) Metaverse governance: an empirical analysis of voting within decentralized autonomous organizations. J Bus Res 160:113764
Gómez S, Mejía D, Tobón S (2021) The deterrent effect of surveillance cameras on crime. J Policy Anal Manag 40(2):553–571
Government Digital Service (2024) Claim compensation if you were the victim of a violent crime. GOV.UK
Guillaume G (2011) The use of precedent by international judges and arbitrators. J Int Disput Settl 2(1):5–23
Gupta D, Jain B, Sharma A (2024) Advancements and challenges in deepfake video detection: a comprehensive review. In: Senjyu T, So-In C, Joshi A (eds.) Smart trends in computing and communications. Springer Nature Singapore, Singapore. pp. 353–369
Guy M, Normand J-M, Jeunet-Kelway C, Moreau G (2023) The sense of embodiment in virtual reality and its assessment methods. Front Virt Real 4:1141683
Hakan Kan C (2024) Criminal liability of artificial intelligence from the perspective of criminal l. Int J Eur Soc Sci 15(55):276–313
Hallevy G (2024) The basic models of criminal liability of AI systems and outer circles. In: Moura Vicente D, Soares Pereira R, Alves Leal A (eds.) Legal aspects of autonomous systems. Springer International Publishing, Cham. pp. 69–82
Harari YN (2018) Sapiens: a brief history of humankind. Harper Perennial, reprint edition
Harff N (2024) Argentina looks to tame crypto market as money-laundering fears draw scrutiny. Reuters
He X, Gong Q, Chen Y, Zhang Y, Wang X, Fu X (2021) Datingsec: detecting malicious accounts in dating apps using a content-based attention network. IEEE Trans Dependable Secur Comput 18(5):2193–2208
Heath A (2021) Meta opens up access to its VR social platform horizon worlds. The Verge
Heirman W, Walrave M, Ponnet K, Gool EV (2013) Predicting adolescents' willingness to disclose personal information to a commercial website: testing the applicability of a trust-based model. Cyberpsychol J Psychosoc Res Cyberspace 7(3)
Henman P (2020) Improving public services using artificial intelligence: possibilities, pitfalls, governance. Asia Pac J Public Adm 42(4):209–221

Hing N, Dittman CK, Russell AMT, King DL, Rockloff M, Browne M et al. (2022) Adolescents who play and spend money in simulated gambling games are at heightened risk of gambling problems. Int J Environ Res Public Health 19(17):10652
Holman EA, Garfin DR, Lubens P, Silver RC (2020) Media exposure to collective trauma, mental health, and functioning: Does it matter what you see? Clin Psychol Sci 8(1):111–124
House of Commons Hansard (2014) Written answers to questions. www.parliament.uk
Huang RH, Deng H, Chan AFL (2023) The legal nature of cryptocurrency as property: Accounting and taxation implications. Comput Law Secur Rev 51:105860
Inaba M, Ukiyo M, Takamizo K (2024) Can large language models be used to provide psychological counselling? An analysis of GPT-4-generated responses using role-play dialogues. https://arxiv.org/abs/2402.12738 (2024)
Inkpen K, Chappidi S, Mallari K, Nushi B, Ramesh D, Michelucci P et al. (2023) Advancing human-AI complementarity: The impact of user expertise and algorithmic tuning on joint decision making. ACM Trans Comput-Hum Interact 30(5):1–29
INTERPOL (2024a) Metaverse: a law enforcement perspective. Technical report, INTERPOL
INTERPOL (2024b) What is Interpol? INTERPOL
Iu KY, Wong VM-Y (2023) The trans-national cybercrime court: towards a new harmonisation of cyber law regime in ASEAN. Int Cybersecur Law Rev 5(1):121–141
Jenkins JP (2024) Prostitution. Britannica
Jiang W (2023) A study of the judicial practice to tackle the virtual property thefts in China today. In: Proceedings of the International Conference on Education, Humanities, and Management (ICEHUM 2022). Atlantis Press. pp. 178–185
Johnson MS (2020) Regulation by shaming: Deterrence effects of publicizing violations of workplace safety and health laws. Am Econ Rev 110(6):1866–1904
JY Tan L (2024) NFT security. Springer Nature Switzerland, Cham, pp. 19–34
Kagan J (2024) Tax evasion: meaning, definition, and penalties. Investopedia
Karaarslan E, Yazici Yilmaz S (2023) Metaverse and decentralization. Springer Nature Singapore, Singapore, p 31–44
Kato R, Kikuchi Y, Yem V, Ikei Y (2022) Reality avatar for customer conversation in the metaverse. In: Yamamoto S, Mori H (eds.) Human interface and the management of information: applications in complex technological environments. Springer International Publishing, Cham. pp. 131–145
Kim S, Kim E (2023) Emergence of the metaverse and psychiatric concerns in children and adolescents. J Korean Acad Child Adolesc Psychiatry 34(4):215–221
Kim YR (2023) Taxing the metaverse. 112 Georgetown Law J (2024, Forthcoming
Kleven H, Landais C, Muñoz M, Stantcheva S (2020) Taxation and migration: evidence and policy implications. J Econ Perspect 34(2):119–42
Knight W (2005) Computer characters mugged in virtual crime spree. NewScientist
Kushwaha N, Roguski P, Watson BW (2020) Up in the air: ensuring government data sovereignty in the cloud. In: 2020 12th International Conference on Cyber Conflict (CyCon), volume 1300, pp. 43–61
Lapidot-Lefler N, Barak A (2012) Effects of anonymity, invisibility, and lack of eye-contact on toxic online disinhibition. Comput Hum Behav 28(2):434–443
Law A (2022) Personal information protection law of the People's Republic of China. PIPL
Law J, Martin EA (2014) Legal person. In: A Dictionary of Law
Le K (2024) Six arrested in cryptocurrency money-laundering scheme in northeast china amid focus on crypto-related capital flows. South Morning China Post
Lee L-H, Braud T, Zhou P, Wang L, Xu D, Lin Z et al. (2021) All one needs to know about metaverse: a complete survey on technological singularity, virtual ecosystem, and research agenda. https://arxiv.org/abs/2110.05352 (2021)
Lee S, Persson P (2022) Human trafficking and regulating prostitution. Am Econ J Econ Policy 14(3):87–127
Leuprecht C, Jenkins C, Hamilton R (2023) Virtual money laundering: policy implications of the proliferation in the illicit use of cryptocurrency. J Financ Crime 30(4):1036–1054
Li B, Lu R, Wang W, Choo K-KR (2016) Ddoa: A dirichlet-based detection scheme for opportunistic attacks in smart grid cyber-physical system. IEEE Trans Inf Forensics Secur 11(11):2415–2425
Li W, Devidze R, Mustafa W, Fellenz S (2024) Ethics in action: training reinforcement learning agents for moral decision-making in text-based adventure games. In: Dasgupta S, Mandt S, Li Y (eds). Proceedings of The 27th International Conference on Artificial Intelligence and Statistics, volume 238 of Proceedings of Machine Learning Research. PMLR. pp. 1954–1962
Lima G, Cha M, Jeon C, Park KS (2021) The conflict between people's urge to punish AI and legal systems. Front Robot AI 8:756242
Liz Jackson, PA Media (2024) Woman found with 2bn euros in bitcoin convicted of money laundering arrangement offence. BBC
López-Torres I, León-Quismondo L, Ibáñez, A (2021) Impulsivity, lack of premeditation, and debts in online gambling disorder. Front Psychiatry 11:618148
Malamuth NM (2018) "Adding fuel to the fire"? does exposure to non-consenting adult or to child pornography increase risk of sexual aggression? Aggression Violent Behav 41:74–89
Malhotra V (2023) That's assault! extension of criminal law to the metaverse. Extension of Criminal Law to the Metaverse. https://ssrn.com/abstract=4595652 (March 2, 2023)
Malik M, Malik MK, Mehmood K, Makhdoom I (2021) Automatic speech recognition: a survey. Multimed Tools Appl 80(6):9411–9457
Marr B (2024) The Metaverse and its dark side: confronting the reality of virtual rape. Forbes
Marshall AM, Tompsett BC (2024) The metaverse—not a new frontier for crime. WIREs Forensic Sci 6(1):e1505
Marshall B (2023) No legal personhood for AI. Patterns 4(11):100861
McIntosh TR, Liu T, Susnjak T, Watters P, Ng A, Halgamuge MN (2024) A culturally sensitive test to evaluate nuanced gpt hallucination. IEEE Trans Artif Intell 5(6):2739–2751
McStay A (2023) The metaverse: surveillant physics, virtual realist governance, and the missing commons. Philos Technol 36(1):13
Merriam-Webster (2024a) Chronological age. In: Merriam-Webster.com dictionary
Merriam-Webster (2024b) Privacy. In: Merriam-Webster.com dictionary
Merriam-Webster (2024c) Prosecution. In: Merriam-Webster.com dictionary
Meta (2023) Meta horizon worlds. Meta
Ministers for the Department of Infrastructure (2023) New mandatory minimum classifications for gambling-like games content. Ministers for the Department of Infrastructure
Montagnani ML, Najjar M-C, Davola A (2024) The EU regulatory approach(es) to AI liability, and its application to the financial services market. Comput Law Secur Rev 53:105984
Mooij A (2024a) Money laundering and financing of terrorism via the Metaverse. Springer Nature Switzerland, Cham, pp. 21–34
Mooij A (2024b) Regulating the technology (Placement). Springer Nature Switzerland, Cham, pp. 35–67
Mukta R, Martens J, Paik H-Y, Lu Q, Kanhere SS (2020) Blockchain-based verifiable credential sharing with selective disclosure. In: 2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). pp. 959–966
Mutimukwe C, Kolkowska E, Grönlund Å (2020) Information privacy in e-service: effect of organizational privacy assurances on individual privacy concerns, perceptions, trust and self-disclosure behavior. Gov Inf Q 37(1):101413
Nicola AD (2021) The differing EU member states' regulations on prostitution and their cross-border implications on women's rights. Technical report, European Parliament's Committee on Women's rights and Gender Equality
Nikkei Staff Writers (2022) Japan cryptocurrency transfer rules take aim at money laundering. Nikkei Asia
Ning H, Wang H, Lin Y, Wang W, Dhelim S, Farha F et al. A survey on metaverse: the state-of-the-art, technologies, applications, and challenges. https://arxiv.org/abs/2111.09673 (2021)
Nix N (2024) Attacks in the metaverse are booming. Police are starting to pay attention. The Washington Post
Noothigattu R, Bouneffouf D, Mattei N, Chandra R, Madan P, Varshney KR (2019) Teaching AI agents ethical values using reinforcement learning and policy orchestration. IBM J Res Dev 63(4/5):2:1–2:9
Nower L, Anthony WL, Stanmyre JF (2022) The intergenerational transmission of gambling and other addictive behaviors: implications of the mediating effects of cross-addiction frequency and problems. Addict Behav 135:107460
Ntoutsi E, Fafalios P, Gadiraju U, Iosifidis V, Nejdl W, Vidal M-E (2020) Bias in data-driven artificial intelligence systems—an introductory survey. WIREs Data Min Knowl Discov 10(3):e1356
Ogbonna N (2024) Nigeria binance dispute: Cryptocurrency official denies money laundering. *BB*
Oleksii K, Oleksii D, Dmytro Z (2024) Metaverse: ensuring legal recognition of avatars and electronic personalities through a cross-border personalized ID-code. Int J Innov Technol Soc Sci 2(42):1–5
Oulasvirta A, Hornbæk K (2022) Counterfactual thinking: What theories do in design. Int J Hum–Comput Interact 38(1):78–92
Padovan PH, Martins CM, Reed C (2023) Black is the new orange: how to determine AI liability. Artif Intell Law 31(1):133–167
Papagiannidis E, Enholm IM, Dremel C, Mikalef P, Krogstie J (2023) Toward AI governance: Identifying best practices and potential barriers and outcomes. Inf Syst Front 25(1):123–141
Peterson C, DeGue S, Florence C, Lokey CN (2017) Lifetime economic burden of rape among u.s. adults. Am J Prev Med 52(6):691–701
Piaget J (2013) The moral judgment of the child. Routledge

Qin HX, Hui P (2023) Empowering the metaverse with generative AI: survey and future directions. In: 2023 IEEE 43rd International Conference on Distributed Computing Systems Workshops (ICDCSW), pp. 85–90
Radin TJ (2024) Identity theft. Britannica
Rahamthaulla MA (2020) A study on internet industry self-regulation in China and its implications for child protection in cyberspace. Int J Community Soc Dev 2(3):297–309
Rahman AS, Pilver CE, Desai RA, Steinberg MA, Rugle L, Krishnan-Sarin S (2012) The relationship between age of gambling onset and adolescent problematic gambling severity. J Psychiatr Res 46(5):675–683
Rashik M, Jasim M, Kucher K, Sarvghad A, Mahyar N (2024) Beyond text and speech in conversational agents: Mapping the design space of avatars. In: Proceedings of the 2024 ACM Designing Interactive Systems Conference, DIS '24, New York, NY, USA. Association for Computing Machinery. pp. 1875–1894
Ratner C (2021) When "sweetie"' is not so sweet: artificial intelligence and its implications for child pornography. Fam Court Rev 59(2):386–401
Raymond JG (2004) Ten reasons for not legalizing prostitution and a legal response to the demand for prostitution. J Trauma Pract 2(3-4):315–332
Reeves C (2018) The virtual simulation of child sexual abuse: online gameworld users' views, understanding and responses to sexual ageplay. Ethics Inf Technol 20(2):101–113
Rehman MHU, Salah K, Damiani E, Svetinovic D (2020) Trust in blockchain cryptocurrency ecosystem. IEEE Trans Eng Manag 67(4):1196–1212
Reingnaum JF (1993) The law enforcement process and criminal choice. Int Rev Law Econ 13(2):115–134
Ren M, Chen N, Qiu H (2023) Human-machine collaborative decision-making: An evolutionary roadmap based on cognitive intelligence. Int J Soc Robot 15(7):1101–1114
Repetto C, Riva G (2024) Editorial "embodiment in the metaverse: How real and virtual bodies in interaction affect cognition". J Cogn 7(1):51
Reuters (2022) EU backs crypto anti-money laundering rules. Reuters
Roblox (2023a) Age ID verification. Roblox. https://en.help.roblox.com/hc/en-us/articles/4407282410644-Age-ID-Verification. Accessed 5 Aug 2024
Roblox (2023b) Roblox. https://www.roblox.com/
Sandalcı U, Sandalcı I (2021) Effect of taxation on migration in the globalization process. J Manag Econ Res 19(1):110–132
Scharfman J (2024) Decentralized Autonomous Organization (DAO) fraud, hacks, and controversies. Springer Nature Switzerland, Cham, pp. 65–106
Schneider N, De Filippi P, Frey S, Tan JZ, Zhang AX (2021) Modular politics: toward a governance layer for online communities. Proc ACM Hum-Comput Interact 5 (CSCW1). https://doi.org/10.1145/3449090
Seo S, Seok B, Lee C (2023) Digital forensic investigation framework for the metaverse. J Supercomput 79(9):9467–9485
Shore A, Prena K, Cummings JJ (2022) To share or not to share: extending protection motivation theory to understand data sharing with the police. Comput Hum Behav 130:107188
Singh A (2023) International deal to combat crypto tax evasion to start 2027 as 48 countries sign up. Coin Desk
Smetana JG, Jambon M (2017) Parenting, morality and social development: new views on old questions. In: New perspectives on moral development. Routledge. pp. 121–140
Soliman MM, Ahmed E, Darwish A, Hassanien AE (2024) Artificial intelligence powered metaverse: analysis, challenges and future perspectives. Artif Intelli Rev 57(2):36
Statista (2024a) Cryptocurrencies—worldwide. Statista
Statista (2024b) Metaverse—worldwide. Statista
Stephenson N (2022) Snow crash. Viking, London, England
Strikwerda L (2012) Theft of virtual items in online multiplayer computer games: an ontological and moral analysis. Ethics Inf Technol 14(2):89–97
Stubbs-Richardson M, Rader NE, Cosby AG (2018) Tweeting rape culture: examining portrayals of victim blaming in discussions of sexual assault cases on Twitter. Feminism Psychol 28(1):90–108
Sudhakar KN, Shanthi M (2023) Deepfake: an endanger to cyber security. In: 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS). IEEE. pp. 1542–1548
Sueur C, Lombard J, Capra O, Beltzung B, Pelé M (2024) Exploration of the creative processes in animals, robots, and AI: who holds the authorship? Humanit Soc Sci Commun 11(1):611
Sukhai NB (2004) Hacking and cybercrime. In: Proceedings of the 1st Annual Conference on Information Security Curriculum Development, InfoSecCD '04, New York, NY, USA. Association for Computing Machinery. pp. 128–132
Suler J (2004) The online disinhibition effect. Cyberpsychol Behav 7(3):321–326
Teichmann F (2020) Recent trends in money laundering. Crime Law Soc Change 73(2):237–247
The Editors of Encyclopaedia Britannica (2023) Citizenship. Britannica. https://www.britannica.com/topic/citizenship. Accessed 30 Dec 2023
The Editors of Encyclopaedia Britannica (2024a) Assault and battery. Britannica. https://www.britannica.com/topic/assault-and-battery. Accessed 14 Aug 2024
The Editors of Encyclopaedia Britannica (2024b) Currency. Britannica. https://www.britannica.com/money/currency. Accessed 5 Aug 2024
The Editors of Encyclopaedia Britannica (2024c) Fiat money. Britannica. https://www.britannica.com/money/fiat-money. Accessed 5 Aug 2024
The Editors of Encyclopaedia Britannica (2024d) Money laundering. Britannica. https://www. britannica.com/ topic/money-laundering. Accessed 5 Aug 2024
The Editors of Encyclopaedia Britannica (2024e) Naturalization. Britannica. https://www.britannica.com/topic/naturalization. Accessed 5 Aug 2024
The Editors of Encyclopaedia Britannica (2024f) Property. Britannica https://www.britannica.com/money/property-legal-concept. Accessed 5 Aug 2024
The Peninsula Online (2021) Bitcoin trading prohibited in Qatar: Central bank. The Peninsula
The World Financial Review (2022) Online gambling laws throughout the world. The World Financial Review
Thommandru A, Chakka DB (2023) Recalibrating the banking sector with blockchain technology for effective anti-money laundering compliances by banks. Sustain Future 5:100107
Tomic S (2022) Regulatory approach to anti-money laundering in online gambling in the UK. Springer International Publishing, Cham, pp. 47–65
United Nations (2024) Money laundering through cryptocurrencies. UN Toolkit on Synthetic Drugs
United Nations Office on Drugs and Crime (2024) Money laundering. United Nations
United Nations Office on Drugs and Crime (2019) Cyberstalking and cyberharassment. United Nations Office on Drugs and Crime
Vellinga NE (2024) Rethinking compensation in light of the development of AI. Int Rev Law Comput Technol 0(0):1–22
Von Ihering R (2009) Law as a means to an end. Kessinger Publishing
Wagner M, Johann D, Kritzinger S (2012) Voting at 16: Turnout and the quality of vote choice. Elect Stud 31(2):372–383. Special Symposium: Generational Differences in Electoral Behaviour
Wang H (2023) How to deal with virtual property crime: Judicial dilemma and a theoretical solution from China. Comput Law Secur Rev 49:105808
Wang N, Zhou J, Li J, Han B, Li F, Chen S (2024a) Hardenvr: Harassment detection in social virtual reality. In: 2024 IEEE Conference Virtual Reality and 3D User Interfaces (VR). IEEE, pp. 94–104
Wang X. Hong Y, He X (2024b) Exploring artificial intelligence generated content (AIGC) applications in the metaverse: challenges, solutions, and future directions. IET Blockchain 1–14
Wang Y, Su Z, Zhang N, Xing R, Liu D, Luan TH et al. (2022) A survey on metaverse: Fundamentals, security, and privacy. IEEE Commun Surv Tutor 25(1):319–352
Wang Y, Su Z, Yan M (2023) Social metaverse: challenges and solutions. IEEE Internet Things Mag 6(3):144–150
Ward A (2009) Ashcroft v. free speech coalition (2002). The First Amendment Encyclopedia. Free Speech Center at Middle Tennessee State University
Weber RH (2015) Realizing a new global cyberspace framework. Springer Berlin, Heidelberg
Wiener JB (2004) The regulation of technology, and the technology of regulation. Technol Soc 26(2):483–500
Wolford B (2024) What is GDPR, the EU's new data protection law? GDPR.EU
Wu H, Zhang W (2023) Digital identity, privacy security, and their legal safeguards in the metaverse. Security Saf 2:2023011
Xiang C (2023). 'He Would Still Be Here': man dies by suicide after talking with ai chatbot, widow says. VICE
Xie J, Yu FR, Huang T, Xie R, Liu J, Liu Y (2019) A survey on the scalability of blockchain systems. IEEE Netw 33(5):166–173
Xu C, Sun Y, Zhong R (2024) The veil of virtuality: anonymity, identity curation, and trust in the metaverse's new frontier. In: Proceedings of the Eleventh International Symposium of Chinese CHI, CHCHI '23, New York, NY, USA. Association for Computing Machinery. pp. 386–403
Yandoli KL (2024) Roblox users can earn more working for Ikea than some real-life employees. RollingStone
Yang K, Zhang Z, Youliang T, Ma J (2023) A secure authentication framework to guarantee the traceability of avatars in metaverse. IEEE Trans Inf Forensics Secur 18:3817–3832
Yang L (2023a) Recommendations for metaverse governance based on technical standards. Humanit Soc Sci Commun 10(1):1–10
Yang L (2023b) Recommendations for metaverse governance based on technical standards. Humanit Soc Sci Commun 10(1):253
Yang L, Xu Y, Hui P (2024) Metaverse identity: core principles and critical challenges. https://arxiv.org/abs/2406.08029 (2024)
Yasin R, Namoco SIO (2021) Prostitution: a new dynamic of discrimination. Gend Manag Int J 36(4):553–567

Yermack D (2024) Chapter 2—Is Bitcoin a real currency? An economic appraisal. In: Lee Kuo Chuen D, (ed.) Handbook of digital currency (second edition). Academic Press, San Diego. pp. 29–40

Zhang Y, Wang T, Hsu C (2020) The effects of voluntary GDPR adoption and the readability of privacy statements on customers' information disclosure intention and trust. J Intellect Cap 21(2):145–163

Zwitter A, Hazenberg J (2021) Cyberspace, blockchain, governance: how technology implies normative power and regulation. In: Cappiello B, Carullo G, (eds) Blockchain, law and governance. Springer International Publishing, Cham. pp. 87–97

Author contributions

HXQ was responsible for the writing of the article. YW and PH supervised the project.

Competing interests

The authors declare no competing interests.

Ethical approval

This article does not contain any studies with human participants performed by any of the authors.

Informed consent

This article does not contain any studies with human participants performed by any of the authors.

Additional information

Correspondence and requests for materials should be addressed to Pan Hui.