




Adnan Hadziselimovic  <https://orcid.org/0000-0001-6862-6745>

Faculty of Media & Knowledge Sciences
University of Malta
Msida, Malta

Krzysztof Pijarski  <https://orcid.org/0000-0002-7121-3607>

Łódź Film School
Łódź, Poland

FREEDOM OF EXPRESSION IN PRIVACY VS. PUBLIC INTEREST, A CASE FOR OPEN JUSTICE IN EXTENDED REALITY¹

Abstract

This paper continues the discussion on advanced jurisprudence, outlined in *Algorithms, Ethics and Justice* (Hadzi, 2022), where restorative justice was proposed for the mitigation of artificial intelligence (AI) crimes. *Algorithms, Ethics and Justice* proposed an alternative approach to the current legal system by looking into restorative justice for AI crimes, and how the ethics of care could be applied to AI technologies. The paper signifies an expanded version of Hadzi's contribution to the Digital Research in Humanities and Art Conference (Hadzi, 2023), focusing on the notion of cyber offenses in extended reality (XR), given the rise of the metaverse (Anderson, Rainie, 2022; Chohan, 2022), and the future scenario of bio-metrical data of EEG capable headsets (Graham, 2022) being misused by rogue companies and/or criminals (Jaber, 2022; Nair et al., 2022; Zhao et al., 2022). The authors begin by questioning the cyberspace – including the emerging metaverse – as public sphere, i.e. a social space in which democracy is being enacted to explore open justice in extended realities (XR), and then by continuing the discussion around the right to be forgotten and the freedom of the press versus privacy, through a comparative analysis between the legal situation in the EU and that of the USA. The paper concludes by warning against excessive state control while attempting to project a desirable scenario of multiple digital public spheres.

¹ The article was developed within the framework of the project “Experience and immersive technologies – from creative practice to educational theory” in partnership with Jagiellonian University, Lodz Film School, University of Malta and University of Athens (project ID number: 2020-1-PL01-KA226-HE-095891).

Keywords: artistic research, augmented reality, extended reality, open justice, privacy, freedom of expression, metaverse, social media

Introduction

A legally well-regulated metaverse (Ravenscraft, 2022; Reinhardt, Warin, 2022), and in a wider sense a well-regulated social media environment, could be seen as a potential democratic tool allowing metaverse users the freedom of expression (UNESCO, 2011) and the freedom of information access (Wagner, 2022), through an advanced form of jurisprudence. Nevertheless, social media users, including metaverse users, should also consider that those rights come with responsibilities, namely legal restrictions on infringing other users' privacy rights (Hartshorne, 2010, p. 69). With social media turning towards extended realities (XR) by creating platforms such as Meta Horizon, VRChat, Sansar, NeosVR, Spatial, etc., a pseudo public space is being created offering a platform for public discourse (Balkin, 2005).

From its very inception, the Internet was lauded as a new form of public space (Papacharissi, 2019), and because it is at once ubiquitous and personal, one defined by seemingly contradictory characteristics (Camp, Chien, 2000). Unlike the traditional media types of broadcast, common carrier, publishing, or distribution and the physical public spaces, such as a commons, a public square or library, the liquidity of the cyberspace makes it difficult to clearly delineate the outline and definite traits of that "information agora" (Branscomb, 1990), "virtual agora" (Toriz Ramos, 2021), or even – as defined by Hilary Clinton in her "Internet freedom" speech from 2011 – the "public space of the 21st century" (MacKinnon, 2011). At the same time, as Zizi Papacharissi explains,

It should be clarified that a new public space is not synonymous with a new public sphere. As public space, the internet provides yet another forum for political deliberation. As public sphere, the internet could facilitate discussion that promotes a democratic exchange of ideas and opinions. A virtual space enhances discussion; a virtual sphere enhances democracy (Papacharissi, 2019, p. 44).

Granted, the Habermasian concept of the "sphere between civil society and the state, in which critical public discussion of matters of general interest was institutionally guaranteed" (Habermas, 1991, p. xi) has faced substantial critique: Chantal Mouffe, for example, countering Habermas' insistence on rational deliberation and consensus, would stress "agonistic pluralism" as core of democratic process (Mouffe, 2000, 2005) and Nancy Fraser – while agreeing that "something like" the idea of the public sphere is "indispensable for critical social theory and to democratic political practice" – insisted on, among others, the necessity of multiple public spheres of subaltern counter-publics and inclusion of interests and issues hitherto labeled as "private" and hence inadmissible, as prerequisites (Fraser, 1990,

p. 57). However, what all these models have in common is a separation between private and public space, a separation that simply cannot be upheld in the context of cyberspace.

As Jean Camp and YT Chien indicate, three issues must be taken into account when attempting to regulate electronic spaces: simultaneity, permeability, and exclusivity (Camp, Chien, 2000). The first refers to the fact that in cyberspace, users can be in several places at once (at home and at work, at work and in the public space of social media, participating in a heated debate for instance, etc.), and the second bespeaks the breaking down of clear-cut boundaries between the different spaces of social life – especially from the contemporary experience of remote work, the barrier between work and home has been attenuated to the degree of non-existence; exclusivity references the fact that the Internet, as we very well know in the wake of its encroaching privatization, commodification, and commercialization (Fuchs, 2021), cannot be defined as an open space, agora, or commons. All these factors determine that in cyberspace, “the public space, the private sector space, and the personal spaces merge seamlessly” (Camp, Chien, 2000, p. 14), it is at the same time private and public space (Papacharissi, 2019). Papacharissi contends that “whereas in the truest iterations of democracy, the citizen was enabled through the public sphere, in contemporary democracy, the citizen acts politically from a private sphere of reflection, expression, and behavior” (Papacharissi, 2009, p. 15). This state of affairs has far-reaching consequences for how to conceptualize the above-mentioned rights and responsibilities.

In one of liberalism’s founding texts, John Stuart Mill gives an apt example on why this is the case. Although Mill could not have had in mind social media influencers versus individual users (as well as today’s concept of “shitstorms”), his example throws into relief the issues of violence and abuse certain social media posts can inflict on parties in cyberspace.

No one pretends – writes Mill – that actions should be as free as opinions. On the contrary, even opinions lose their immunity when the circumstances in which they are expressed are such as to constitute their expression a positive instigation to some mischievous act. An opinion that corn dealers are starvers of the poor, or that private property is robbery, ought to be unmolested when simply circulated through the press, but may justly incur punishment when delivered orally to an excited mob assembled before the house of a corn dealer, or when handed about among the same mob in the form of a placard. Acts, of whatever kind, which without justifiable cause do harm to others may be, and in the more important cases absolutely require to be, controlled by the unfavourable sentiments, and, when needful, by the active interference of mankind (Mill, 1978, p. 41).

On the Internet, especially on social media, we are rarely exclusively private persons, but very often, at the same time, pamphleteers, broadcasters, publishers, distributors, sometimes even to the point of inciting mobs. A recent study by Karsten Müller and Carlo Schwarz has in a convincing way established a correlation between the social media activity of the German right-wing party Alternative

für Deutschland (AfD) and hate crimes in Germany. Their study implies that “in the absence of anti-refugee posts on the AfD Facebook page 446 (13%) fewer anti-refugee incidents would have taken place”, therefore trenchantly illustrating the permeability between opinion and action on social media (Müller, Schwarz, 2018, p. 41). The Dutch town of Bodegraven, whose cemetery was overrun in 2021 by supporters of a QAnon-inspired conspiracy involving a satanic pedophile ring and trying to implicate the prime minister and a prominent Dutch virologist, tells the same story. In a turn important in the context of this argument, the main instigators of the conspiracy were arrested and convicted, the platforms they used shut down – the two Telegram channels they operated had 13.000 members in total (Meaker, 2023), which gives an idea about the impact of this seemingly fringe narrative.

Concluding these opening remarks, we would like to argue that as regards cyberspace it is exactly the relationship between privacy and public interest that is among today’s most urgent issues of real democracy. And not only because of the impact private individuals can have in public matters – for better or for worse – but also, in response to the possible effects of this seemingly unbridled access, because of the ways the custodians of online social life, both corporate and governmental, try to control this relay, often to the point of invading their privacy.

The question of XR and the Metaverse

How does all this translate into the relatively new spaces of the metaverse, the emergent world of online collective virtual shared XR spaces? First, the development of cyberspace towards immersive spaces further bolsters the space metaphor as regards the Internet (rather understanding it as a medium), throwing into stark relief the need to look closer at the distinction between private and public. This is all the more so, because immersive spaces – while retaining the trait of permeability (we can be at home and at the same time at a town hall meeting or an exhibition opening) – are no longer, or in a much more constrained way, simultaneous: when immersed in a virtual space with other people, we are no longer able to be at the same time on Facebook, Instagram, Twitter, etc. This characteristic, on the other hand, tethers us to a given immersive space, makes us much more present, and therefore more likely to experience copresence and to open up to the others, which is supported by recent research. In immersive space a certain aspect of anonymity is preserved: we do not need to care, or worry, how we look (because we have an avatar as a stand-in), we do not need to control our facial expressions etc., and so we can focus on the interaction as such (Bradbury, 2021). At the same time, if our avatar resembles a human person, it elicits reactions “that would be appropriate only in the presence of a real human” (Bailenson et al., 2005, p. 390). What is more, an avatar is both an object (different from our self) and a persona (a projection of self). Hence, as indicated by Lesley Procter, “due to the interaction of parasociality, immersion,

and identity, the avatar-persona and user cease to be separate entities” (Procter, 2021, p. 60). While still more research is needed to “fully explore the psychological effects of using VR” in social communication (Bradbury, 2021, p. 66), we could conclude that while the metaverse, at least for now, is not a space of mass gatherings and mass impact (although this is only a question of time if we think of concerts in “Fortnite”, for example), it is a space, where we are much more vulnerable as persons, hence the need to define, and protect, the privacy of metaverse denizens.

While there are still no robust procedures, guidelines, regulations in place about how to deal with today’s flood of fake and inflammatory news spread through social media posts, we need to ask ourselves, how and in what form these issues will (re)appear in the metaverse, a social media environment dominated and molded by powerful companies (Wieshofer, 2022), and what kind of tools in the realm of jurisprudence will be needed to alleviate or remedy their effects? For example, what could be the effects of identity theft, given the role avatars assume for persons, especially in the context of deepfakes. As the authors of a recent paper underline,

unlike the physical world, where impersonating someone convincingly is challenging, it is much easier to create a convincing digital clone of a person in the metaverse due to the abundance of personal information available on the internet that can be used to create deepfakes (Tariq et al., 2023).

The possibility of impersonation and/or identity theft leads to the danger of (loss of) reputation, assault, hate speech, etc. One possible answer to what might be considered a central threat in the development of the metaverse could be Decentralized Identifiers, since last year an official Web standard: a new type of persistent identifier for individuals and organizations that does not require any central registry, and allows the stakeholders to take greater control of their “online information and relationships, while also providing greater security and privacy” (*Decentralized Identifiers (DIDs) v1.0 Becomes a W3C Recommendation*, 2022).

Returning to Mill for a moment, one might say that if we are able to guarantee free and open social media – and as we know, it is private actors who exercise almost all control over internet speech, which is part of the problem (Abbasi, 2017) – they would, in principle, allow for the establishing of truth through fact finding and public discourse, analyzing the false or fake information published or enunciated (Parialò, 2022). Furthermore Mill’s position would be strongly against majorities’ preconceptions and biases being intrusive on individual users’ “social graces” (i.e. aspects of personal and social identity such as gender, religion, ability, class, ethnicity or sexuality [Burnham, 2012]). In a perfect virtual world, public discussion would offer a sound judgment. It is in the public interest to establish truth. Public interest, according to Denis McQuail, can be understood as a “complex of supposed informational, cultural and social benefits to the wider society, which go beyond the immediate, particular and individual interests of those who participate in public communication, whether as senders or receivers” (McQuail, 1992, p. 11). It

is a concept, as Zrinjka Peruško underlines, “linked to the contribution of the media to the development of a democratic public sphere”, which brings us back to the basic tenet of these considerations (Peruško, 2009, p. 7).

Privacy and public interest

In European Union member states’ courts, public interest and freedom of expression – as already established, key to “open justice” with respect to offenses in cyberspace – are balanced against the right to privacy, and other human rights (Bayer, 2022). The Human Rights Act (*European Convention on Human Rights*, 1998), powerfully impacted European Union jurisdiction, notably in the above mentioned balancing act between the right to privacy (article eight of the Human Rights Act) and freedom of expression (article ten of the Human Rights Act), as well as the right to life (article two of the Human Rights Act). The Parliamentary Assembly of the Council of Europe reaffirmed “the importance of every person’s right to privacy, and of the right to freedom of expression, as fundamental to a democratic society. These rights are neither absolute nor in any hierarchical order, since they are of equal value” (Parliamentary Assembly, 1998; Christie, Tugendhat, 2002).

Freedom of expression, on the other hand, allows for an open justice system, through which public interest is safeguarded and fair trials can be conducted. Nevertheless, certain offenders may need protection from extrajudicial attacks, due to the nature of their offenses. It has been argued that the balancing act of European Courts has led to a decline of open justice, due to freedom of expression being “pitched” against privacy rights and the right to a fair trial (Abramovsky et al., 1993), as well as the right to life. In this connection, a famous case, which upheld the right to privacy (Dyer, Hall, 2002), serving as a reference for privacy rights safeguarding against offenses in cyberspace (and the metaverse), was Naomi Campbell’s court case against the “Daily Mirror” (*Campbell (Apellant) v. MGN Limited (Respondents)*, 2004), who pictured her in front of a drug rehabilitation facility. The court granted Campbell right to privacy overriding the newspaper’s right to freedom of expression. With respect to the protection of privacy, the court noted:

...the fundamental importance of protecting private life from the point of view of the development of every human being’s personality. That protection (...) extends beyond the private family circle and also includes a social dimension. The Court considers that anyone, even if they are known to the general public, must be able to enjoy a “legitimate expectation” of protection of and respect for their private life (*Campbell (Apellant) v. MGN Limited (Respondents)*, 2004).

The court’s ruling meant that the freedom of expression was circumscribed in favor of the right to privacy, because the information divulged, as one might argue here, had nothing to do with public interest. Lord Steyn, in a case relating

to restrictions on publication, stated, referring to articles 8 and 10 of the Human Rights Act, that “first, neither article has precedence as such over the other. Secondly, where the values under the two articles are in conflict, an intense focus on the comparative importance of the specific rights being claimed in the individual case is necessary. Thirdly, the justification for interfering with each right must be taken into account. Finally, the proportionality test must be applied to each. For convenience I will call this the ultimate balance test” (*Re S (A Child)*, 2005). Lord Nicholls continued the argumentation in the *Campbell* case, stating that “freedom of expression has been stressed often and eloquently, the importance of privacy less so. But it, too, lies at the heart of liberty in a modern state. A proper degree of privacy is essential for the well-being and development of an individual. And restraints imposed on the government to pry into the lives of the citizen go to the essence of a democratic state” (*Campbell (Appellant) v. MGN Limited (Respondents)*, 2004).

In the case of possible XR offenses, involving areas like Data Protection, Intellectual Property, Cybersecurity, Sexual Offences, and Social Risks (Bede Chigbogu, Ewulum, 2022), metaverse users could claim “public interest” in order to report on private matters, and especially in virtual space these kind of claims should be scrupulously weighed against the right to privacy. At the same time, it is still not entirely clear what the right to privacy means in the metaverse. In the case *Von Hannover v. Germany* the European Court of Justice ruled that privacy includes “a person’s name, photo or physical and moral integrity” (Global Freedom of Expression, 2004). Moreover, the European Court of Human Rights, referencing article eight, stated “that the notion of personal autonomy is an important principle underlying the interpretation of its guarantees” (*Pretty v. the United Kingdom*, 2002). Interestingly for metaverse users, the notion of reputation was included in article eight of the European Convention on Human Rights (Feldman, 1997), as according to John Zelezny “reputation is what a person is seen to be in the eyes of others – the individual’s projection of self within a society” (Zelezny, 2010, p. 116). As Justice Stewart put forward, “the right of a man to the protection of his own reputation from unjustified invasion and wrongful hurt reflects no more than the basic concept of the essential dignity and worth of every human being; a concept at the root of any decent system of ordered liberty” (Henry, 2021), to which Justice Erickson added that “defamatory statements are so egregious and intolerable because the statement destroys an individual’s reputation; a characteristic which cannot be bought, and one that, once lost, is extremely difficult to restore” (Henry, 2021).

In order to limit freedom of expression in the metaverse there must be concrete evidence of damage to the reputation of a single user. In cyberspace, and one can imagine the same dynamic in the metaverse, influencers often publish information and opinions motivated by likes and profit, and not necessarily by serving public interest. Such users can harm other users by attacking their privacy and reputation. Following articles 8 and 10 of the Human Rights Act requires courts subject to this legislation to strike a balance between the rights to privacy and to self-expression

respectively. The decision of the Court of Appeal in *A v. B Plc and Another* in 2002 reflected on this state of affairs:

The manner in which the two articles operate is entirely different. Article 8 operates so as to extend the areas in which an action for breach of confidence can provide protection for privacy. It requires a generous approach to the situations in which privacy is to be protected. Article 10 operates in the opposite direction. This is because it protects freedom of expression and to achieve this it is necessary to restrict the area in which remedies are available for breaches of confidence. There is a tension between the two articles which requires the court to hold the balance between the conflicting interests they are designed to protect. This is not an easy task but it can be achieved by the courts if, when holding the balance, they attach proper weight to the important rights both articles are designed to protect. Each article is qualified expressly in a way which allows the interests under the other article to be taken into account (*A v B Plc and Another*, 2002).

Such a “balancing act” would be required for XR offenders who, once they have served their sentence (however the punishment will come to be defined), ideally should be rehabilitated. This rehabilitation, however, may involve certain limitations, for example by curtailing freedom of expression, especially if mental health issues are involved, as metaverse users may be disseminating hate speech, causing harm to individual users. Undoubtedly metaverse users have the right to discuss any matter of public interest in the public sphere; however when the right to freedom of expression is misused to spread hate and false stories (Ricardo, 2022) in the pursuit of likes and subscriptions, that right should be restricted and regulated. An example for such need of protection is that of the Maxine Carr “witch hunt” (*Carr v News Group Newspapers Ltd & Others*, 2004), documented in the First Cut TV series entitled *Being Maxine Carr* (Ginnane, 2008). The film shows how women who have been mistaken for Maxine Carr – the woman who provided child murderer Ian Kevin Huntley with a false alibi – were attacked violently, with some women even having to abandon their homes and neighborhoods. For XR offenders, once they have served their sentence – however it will be defined (i.e. as a ban to enter the metaverse for several years) – they should be allowed to return back to society (in this case: the social space of the metaverse) where, under the rule of law, they have the right to privacy and to be left alone. If this proves to be impossible, due to attacks from the public, a controversial “contra mundum” injunction may be enacted, giving the XR offender a new identity, undermining open justice principles. All this presupposes some kind of persistent identifier for the person “inside” the avatar, such as the DID mentioned above, as it appears cyberspace, in light of the many dangers for individual persons, is headed in this direction. Understandably, the public may be afraid of convicted XR offenders joining their communities. Those communities may turn to vigilante self-defence justice, taking the law into their own hands, committing an offense themselves. Compared with the EU, the situation in the USA is very different. In the USA freedom of expression is a constitutional right that overwrites all other rights. There is no balancing act to be

performed between the right to privacy and the right to freedom of expression, of the kind faced by judges in the EU. Thus public interest is defined by users themselves, as manifested in the case *Richmond Newspapers, Inc v. Virginia*, where a judge's decision to close a criminal court case to the public was overruled by the Supreme Court on the count that – based on the First Amendment – “criminal trials must be open to the public unless there is evidence to support an overriding countervailing interest” (*Richmond Newspapers, Inc. v. Virginia*, 1980). Comparably, The Judicial Studies Board, established in the UK in order to protect judicial independence, advises, as a general rule on reporting, which could include social media posts, that “the administration of justice must be done in public. If the court is asked to exclude the media or prevent them from reporting anything, however informally, do not agree to do so without first checking whether the law permits the court to do so... (...) [T]he prime concern is the interests of justice” (Judicial Studies Board, 2009).

At the same time, the practicing of open justice becomes more and more cumbersome in the contemporary world of social media influencers, who are often not clear on whether they are posting for profit, or with a genuine motivation in supporting open justice. For Bohlander, “the debate has been too much about terminological facades in many judicial fora, up to the European Court of Human Rights, for far too long” (Bohlander, 2010, p. 327), and for Crook “reporting of trials inevitably involves an exploitation of the infotainment dimension of journalistic narrative” (Crook, 2009, pp. 263–264). The courts may consider not allowing social media reporters to report about the proceedings, deciding on a case-to-case basis, according to the balancing act (article eight vs. article ten) as set out by the European Convention on Human Rights. This is also where XR offenders are protected through article six of the Human Rights Act, the right to a fair trial, in order to avoid trial by social media. For Abramovsky it “is ironic (...) that while a jury is repeatedly admonished in all cases to consider only the evidence and exhibits which emanate from the witness stand, they are subjected to a barrage of often inflammatory and irrelevant information prior to their impanelment” (Abramovsky et al., 1993, p. 293). At the same time, Bohlander opines that “open court proceedings and the publicity given to criminal trials are vital to the deterrent purpose behind criminal justice. Any departure from the open justice principle must be necessary in order to be justified” (Bohlander, 2010, p. 322), as anonymity might allow for XR offenders, especially given the malleability of the metaverse environment, to “use anonymity to act scandalously or perpetuate skullduggery” (Berryman, 2014, p. 26), to the extent that allowing XR offenders to exploit the system to stay anonymous could result in a culture of mistrust and cast a shadow over whole communities of metaverse users (Gardham, Whitehead, 2010). European Union courts, due to focusing more and more on the right to privacy, are limiting open justice, compared to the USA, which implies limiting what one is allowed to publish on social media, in our case the metaverse. This can lead to a censoring, or even self-censoring, of

metaverse users, who do not take up their right to freedom of speech, despite being protected through article ten (freedom of expression) in the European Convention for the Protection of Human Rights and Fundamental Freedoms (Council of Europe, 2022), as discussed above.

Habeas data

In order to address the notion of open justice within XR environments such as the metaverse one additional concept should be discussed, that of “habeas data” (Fari-var, 2018). Latin for “you have the data”, it stands for the right to collect data (Corrales Compagnucci et al., 2022) and the freedom to delete it. Within digital networks and data centers, the data of individual users is being stored, possibly forever, making it difficult for XR offenders to ever rehabilitate their image. This right was entrenched in EU legislation by the European Union Court of Justice as the “right to be forgotten” in May 2014 (*Google Inc. v Agencia Española de Protección de Datos (AEPD)*, 2014). The Court of Justice of the European Union press release states that “if, following a search made on the basis of a person’s name, the list of results displays a link to a web page which contains information on the person in question, that data subject may approach the operator directly and, where the operator does not grant his request, bring the matter before the competent authorities in order to obtain, under certain conditions, the removal of that link from the list of results” (Court of Justice of the European Union, 2014a). The “right to be forgotten” (Court of Justice of the European Union, 2014b) is a significant right for metaverse users, and not only a “get away” right for XR offenders, considering the vast amount of data which is harvested by data processors from the users – separated from them to the extent of becoming autonomous – and especially the amount of data created, often unwillingly, by users, feeling compelled to share updates about their private affairs on these platforms.

All the platforms making metaverse experiences accessible (Braud et al., 2022) are regarded as both controllers and processors of data under the “right to be forgotten”, and thus have to give metaverse users the right for their data to be removed from said platforms, as already established in the EU 1995 Data Protection Directive (European Data Protection Supervisor, 1995). The legislation applies to any company or data processing operator that “[has] a branch or subsidiary in a Member State which promotes the selling of advertising space” (Venice Commission, 2014, p. 3). In article twelve, the European Court of Justice instructs every member state to ensure that users’ rights are being upheld, obliging data processors to enact “as appropriate the rectification, erasure or blocking of data the processing of which does not comply with the provisions of this Directive, in particular because of the incomplete or inaccurate nature of the data” (European Data Protection Supervisor,

1995). Through the General Data Protection Regulation (GDPR) the “right to be forgotten” now also applies to XR environments, though now referred to as “right to erasure” in article 17 of the GDPR (Logemann, 2018). One also needs to highlight that the GDPR changed from the notion that data belongs to the data processors (and users have to opt-out of data sharing) to data belonging to the users (and users can opt-in to data sharing), meaning that the platforms in question now have to ask for the permission of its users to store personal data of its users in the metaverse.

Concluding remarks

US Supreme Court Judge Brennan called for (social) media to support courts in practicing open justice. Social media posts do not cover all court hearings but select what is in the public interest. Here courts and (social) media reporters often clash on what counts as “public interest”. Social media users feel entitled to report on what they deem to be of importance, while judges have the duty to protect XR offenders to guarantee a fair trial, which for social media users represents a form of censorship and a curtailing of open justice principles. According to Roderick, “research in the United Kingdom and the United States suggests that, more often than not, the [social] media report extraordinary, newsworthy proceedings and tend to ignore ordinary, routine cases that may have educative value” (Rodrick, 2014, p. 135). Social media users are under pressure to gain subscribers for their feeds against their competitors, and thus chase the more sensationalist court hearings, often neglecting rigorous fact checking, meaning that the process of justice is often neglected in favor of reporting on thrilling situations instead. It seems that social media users are focusing mostly on seeking attention and profits. Through the Human Rights Act 1998, European Union courts, and Strasbourg jurisprudence, have become inclined to favor the right to privacy over the right to freedom of expression. Naomi Campbell, as discussed above, was photographed in a public space, when leaving the rehabilitation center, still the judge decided in her favor, overriding the “Daily Mail’s” right to freedom of expression with Campbell’s right to privacy. This ruling is unique to the European Union, because in the USA freedom of speech would carry the day, and a judge would never rule against freedom of expression. In the USA social media users can choose what to report on, and what is in the public interest. It becomes more of an ethical decision for social media users in the USA what to report on. Likewise, the above discussed “contra mundum” injunctions for XR offenders, due to potential attacks of members of the general public against them, could hinder the general public in forgiving those offenders. If the public does not accept former XR offenders, once they served their punishment, society becomes stymied with an archaic criminal justice system. Thus, open justice is an important tool allowing for society to have certainty that XR offenders are being successfully punished and, more importantly, rehabilitated and re-integrated into society.

Freedom of expression and freedom of speech allow for this to happen in a democratic society. Giving the users the right to be forgotten gives them, in fact, the power to enact a “contra mundum” injunction on their own terms, opening up the whole set of issues discussed above. One could ask, how can this impact open justice in the EU (compared to the USA, where freedom of speech trumps privacy rights)?

Freedom of speech also allows for harmful speech, which often infringes on the individual users’ right to privacy and the right to be left alone. At the same time, Deloire from Reporters Without Borders, states that “any movement towards state control would be seen as detrimental to a (...) free press and would send out the wrong message to authoritarian governments” (Deloire, 2012). It is plausible to restrain abuse of power through the public interest defense. Nevertheless, if the definition of such public interest is in the hands of state powers, and the jurisdiction itself, then society moves towards diminishing open justice systems. In an ideal world, XR users would have a balanced discussion on political issues in the public space of the metaverse, producing a form of (multiple & competing) digital public spheres. Rather than following such an idealistic vision, it might be more compelling and adequate to call for a plurality of media within the metaverse. That said, there are certainly also metaverse users who will never breach an ethical code, but those same users might also never risk sharing controversial views, basically conducting self-censorship. This might very well be the new tendency metaverse users see themselves following through future XR criminal court proceedings.

Bibliography

- A v B Plc and Another* (2002). Court of Appeal. <https://vlex.co.uk/vid/v-b-plc-and-793097577> (accessed: 10.03.2024).
- Abbasi S.G. (2017). “Internet as a Public Space for Freedom of Expression: Myth or Reality?”. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.3064175>.
- Abramovsky A., Brook H.R., Cohen J.A., Freeman G., Goodale J.C., Schulz D.A., Schurr C. (1993). “Impact of the Media on Fair Trial Rights: Panel on Media Access”. *Fordham Intellectual Property, Media and Entertainment Law Journal*, 3 (2), p. 291.
- Abuadba A., Moore K., Tariq S. (2023). “Deepfake in the Metaverse: Security Implications for Virtual Gaming, Meetings, and Offices”. arXiv:2303.14612 <http://arxiv.org/abs/2303.14612> (accessed: 10.03.2024).
- Anderson J., Rainie L. (2022). *The Metaverse in 2040*. Washington: Pew Research Center.
- Bailenson J.N., Blascovich J., Dimov A., Hoyt C., Persky S., Swinth K. (2005). “The Independent and Interactive Effects of Embodied-Agent Appearance and Behavior on Self-Report, Cognitive, and Behavioral Markers of Copresence in Immersive Virtual Environments”. *Presence: Teleoperators and Virtual Environments*, 14 (4), pp. 379–393. <https://doi.org/10.1162/105474605774785235>.

- Balkin J.M. (2005). "Digital speech and democratic culture: A theory of freedom of expression for the information society". In: A.D. Moore (ed.). *Information Ethics: Privacy, Property, and Power*. Washington: University of Washington Press.
- Bayer J. (2022). "Procedural rights as safeguard for human rights in platform regulation". *Policy & Internet* (n/a). <https://doi.org/10.1002/poi3.298>.
- Bede Chigbogu A., Ewulum C. (2022). *The Metaverse and the Extended Reality; Examining the Concerns of a Legal Practitioner* (SSRN Scholarly Paper No. 4196187). <https://doi.org/10.2139/ssrn.4196187>.
- Berryman J.B. (2014). "Injunctions contra mundum: The ultimate weapon in containment". *Intellectual Property Journal*, 26 (3), p. 287.
- Bohlander M. (2010). "Open Justice or Open Season?: Should the Media Report the Names of Suspects and Defendants?". *The Journal of Criminal Law*, 74 (4), pp. 321–338. <https://doi.org/10.1350/jcla.2010.74.4.646>.
- Bradbury A.E. (2021). *How Does Virtual Reality Compare? The Effects of Digital Communication Medium and Avatar Appearance on Self-Disclosure*. Raleigh: North Carolina State University. <https://dl.acm.org/doi/book/10.5555/AAI28973096>.
- Branscomb L.M. (1990). "Public Uses of Information Systems: Principles for Design & Application". *International Journal on Human-Computer Interaction*, 2 (2), pp. 173–182.
- Braud T., Hui P., Lee L.H., Zhou P. (2022). "What is the Metaverse? An Immersive Cyberspace and Open Challenges". arXiv:2206.03018. <https://doi.org/10.48550/arXiv.2206.03018>.
- Burnham J. (2012). "Developments in Social GRRRAACCEEESS: Visible–invisible and voiced–unvoiced". In: I.B. Krause (ed.). *Culture and Reflexivity in Systemic Psychotherapy: Mutual Perspectives*. London: Routledge.
- Camp J., Chien Y.T. (2000). "The internet as public space: Concepts, issues, and implications in public policy". *ACM SIGCAS Computers and Society*, 30 (3), pp. 13–19. <https://doi.org/10.1145/572241.572244>.
- Campbell (Appellant) v. MGN Limited (Respondents)* (2004). House of Lords. <https://publications.parliament.uk/pa/ld200304/ldjudgmt/jd040506/campbe-1.htm> (accessed: 10.03.2024).
- Carr v News Group Newspapers Ltd & Others* (2004). Queen's Bench Division. <https://www.5rb.com/case/carr-v-news-group-newspapers-ltd-others/> (accessed: 10.03.2024).
- Chohan U.W. (2022). *Metaverse or Metacurse?* (SSRN Scholarly Paper No. 4038770). <https://doi.org/10.2139/ssrn.4038770>.
- Christie I., Tugendhat M. (2002). *The Law of Privacy and the Media*. Oxford: Oxford University Press.
- Corrales Compagnucci M., Fenwick M., Haapio H., Vermeulen E.P. (2022). "Integrating law, technology, and design: Teaching data protection and privacy law in a digital age". *International Data Privacy Law*, 12 (3), pp. 239–252.
- Council of Europe. (2022). *Convention for the Protection of Human Rights and Fundamental Freedoms*. Impact of the European Convention on Human Rights. <https://www.coe.int/en/web/impact-convention-human-rights/convention-for-the-protection-of-human-rights-and-fundamental-freedoms> (accessed: 10.03.2024).
- Court of Justice of the European Union (2014a). *Court of Justice of the European Union – PRESS RELEASE No 70/14*. <https://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070en.pdf> (accessed: 10.03.2024).
- Court of Justice of the European Union (2014b). *Factsheet on the "Right to be Forgotten" ruling (C-131/12)*. https://web.archive.org/web/20140708142544/http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_data_protection_en.pdf (accessed: 10.03.2024).
- Crook T. (2009). *Comparative Media Law and Ethics*. London: Routledge.

- Decentralized Identifiers (DIDs) v1.0 becomes a W3C Recommendation* (2022). <https://www.w3.org/2022/07/pressrelease-did-rec.html> (accessed: 10.03.2024).
- Deloire C. (2012). *Independence and pluralism must remain central to media regulation*. Reporters Without Borders. <https://rsf.org/en/independence-and-pluralism-must-remain-central-media-regulation> (accessed: 10.03.2024).
- Dyer C., Hall S. (2002). *Legal landmark as Naomi Campbell wins privacy case*. <https://www.theguardian.com/media/2002/mar/28/pressandpublishing.privacy4> (accessed: 10.03.2024).
- European Convention on Human Rights* (1998). Testimony of European Court of Human Rights. https://www.echr.coe.int/Documents/Convention_ENG.pdf (accessed: 10.03.2024).
- European Data Protection Supervisor (1995). *Directive 95/46/EC*. European Union. https://edps.europa.eu/data-protection/our-work/publications/legislation/directive-9546ec_en (accessed: 10.03.2024).
- Farivar C. (2018). *Habeas Data: Privacy vs. the Rise of Surveillance Tech*. New York: Melville House.
- Feldman D. (1997). "The developing scope of Article 8 of the European Convention on Human Rights". *European Human Rights Law Review*, pp. 265–274.
- Fraser N. (1990). "Rethinking the Public Sphere: A Contribution to the Critique of Actually Existing Democracy". *Social Text*, 25/26, p. 56. <https://doi.org/10.2307/466240>.
- Fuchs C. (2021). "The Digital Commons and the Digital Public Sphere How to Advance Digital Democracy Today". *Westminster Papers in Communication and Culture*, 16 (1). <https://doi.org/10.16997/wpcc.917>.
- Gardham D., Whitehead T. (2010). *Terror suspect exploit system to stay anonymous*. <https://www.telegraph.co.uk/news/uknews/law-and-order/7086051/Terror-suspect-exploit-system-to-stay-anonymous.html> (accessed: 10.03.2024).
- Garrido G.M., Nair V., Song D. (2022). "Exploring the Unprecedented Privacy Risks of the Metaverse". arXiv:2207.13176. <https://doi.org/10.48550/arXiv.2207.13176>.
- Ginnane M. (dir.) (2008). *Being Maxine Carr* [documentary]. Renegade Pictures.
- Global Freedom of Expression (2004). *Von Hannover v. Germany (No. 2)*. <https://global-freedomofexpression.columbia.edu/cases/von-hannover-v-germany-no-2/> (accessed: 10.03.2024).
- Google Inc. V Agencia Española de Protección de Datos (AEPD)* (2014). European Union Court of Justice. https://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&docid=152065 (accessed: 10.03.2024).
- Graham P. (2022). *Muse Set to Launch a VR Compatible EEG Headband*. <https://www.gmw3.com/2022/03/muse-set-to-launch-a-vr-compatible-eeeg-headband/> (accessed: 10.03.2024).
- Habermas J. (1991). *The Structural Transformation of the Public Sphere: An inquiry Into a Category of Bourgeois Society* (T. Burger, trans.). Cambridge: The MIT Press.
- Hadzi A. (2022). "Algorithms, Ethics and Justice". In: S. Bezzina, M. Bugeja, A. Dingli, A. Pfeiffer, A. Serada (eds.). *Disruptive Technologies in Media, Arts and Design* (pp. 121–138). New York: Springer International Publishing. https://doi.org/10.1007/978-3-030-93780-5_9.
- Hadzi A. (2023). "Open justice transformations impacting extended reality (XR) environments". *International Journal of Performance Arts and Digital Media*, 19 (1), pp. 121–138. <https://doi.org/10.1080/14794713.2023.2198535>.
- Hartshorne J. (2010). "The Value of Privacy". *The Journal of Media Law*, 2 (1), pp. 67–84. <https://doi.org/10.1080/17577632.2010.11427354>.
- Henry B. (2021). *Online Defamation and Your Business*. <https://www.robinsonandhenry.com/legal-guides/online-defamation-and-your-business/> (accessed: 10.03.2024).

- Hua Z., Lan R., Zhang Y., Zhao R., Zhu Y. (2022). "Metaverse: Security and Privacy Concerns". arXiv:2203.03854. <https://doi.org/10.48550/arXiv.2203.03854> (accessed: 10.03.2024).
- Jaber T.A. (2022). "Security Risks of the Metaverse World". *International Journal of Interactive Mobile Technologies*, 16 (13).
- Judicial Studies Board (2009). *Reporting Restrictions in the Criminal Courts*. <https://www.judiciaryni.uk/> (accessed: 10.03.2024).
- Logemann T. (2018). *Art. 17 GDPR – Right to erasure ('right to be forgotten') – General Data Protection Regulation (GDPR)*. Intersoft Consulting. <https://gdpr-info.eu/art-17-gdpr/> (accessed: 10.03.2024).
- MacKinnon R. (2011). 'Internet Freedom' in the Age of Assange. <https://foreignpolicy.com/2011/02/17/internet-freedom-in-the-age-of-assange/> (accessed: 10.03.2024).
- McQuail D. (1992). *Media Performance: Mass Communication and the Public Interest*. Thousand Oaks: Sage Publications.
- Meaker M. (2023). *This Town Became the Center of a QAnon Storm. It's Fighting Back*. <https://www.wired.com/story/qanon-conspiracy-bodegraven-netherlands/> (accessed: 10.03.2024).
- Mill J.S. (1978). *On Liberty* (E. Rapaport, ed.). Indianapolis: Hackett Publishing Company, Inc.
- Mouffe Ch. (2000). *The Democratic Paradox*. London–New York: Verso Books.
- Mouffe Ch. (2005). *On the Political*. London: Routledge.
- Müller K., Schwarz C. (2018). "Fanning the Flames of Hate: Social Media and Hate Crime". *Journal of the European Economic Association*, 19 (4), pp. 2131–2167. <https://academic.oup.com/jeea/article-abstract/19/4/2131/5917396?redirectedFrom=fulltext> (accessed: 10.03.2024).
- Papacharissi Z. (2009). "The virtual sphere 2.0: The internet, the public sphere, and beyond". In: A. Chadwick, P.N. Howard (eds.). *Routledge Handbook of Internet Politics* (pp. 230–245). London: Routledge.
- Papacharissi Z. (2019). "The Virtual Sphere. The Internet as a Public Sphere". In: M. Stempfhuber, E. Wagner (eds.). *Praktiken der Überwachen: Öffentlichkeit und Privatheit im Web 2.0* (pp. 43–60). Wiesbaden: Springer Fachmedien Wiesbaden. <https://doi.org/10.1007/978-3-658-11719-1> (accessed: 10.03.2024).
- Parialò A. (2022). *Deepfakes: Analysis on the role of disclosure placement in consumers' attitude towards synthetic advertisement* [Master's Degree Thesis]. Luiss Guido Carli. <http://tesi.luiss.it/32847/>.
- Parliamentary Assembly (1998). *Right to privacy*. <https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=16641&lang%20=en> (accessed: 10.03.2024).
- Peruško Z. (2009). "Public Interest and Television Performance in Croatia". *Medijska Istraživanja: Znanstveno-Stručni Časopis za Novinarstvo i Medije*, 15 (2), pp. 5–31.
- Pretty v. The United Kingdom* (2002). Council of Europe.
- Procter L. (2021). "I Am/We Are: Exploring the Online Self-Avatar Relationship". *Journal of Communication Inquiry*, 45 (1), pp. 45–64. <https://doi.org/10.1177/0196859920961041>.
- Ravenscraft E. (2022). *What Is the Metaverse, Exactly?* <https://www.wired.com/story/what-is-the-metaverse/> (accessed: 10.03.2024).
- Reinhardt D., Warin C. (2022). "Vision: Usable Privacy for XR in the Era of the Metaverse". *Proceedings of the 2022 European Symposium on Usable Security*, pp. 111–116. <https://doi.org/10.1145/3549015.3554212>.
- Re (S) (*A child*) (2005). Court of Appeal (Civil Division). <https://www.4pb.com/pdf.php?id=2888> (accessed: 10.03.2024).

- Ricardo Q.S. (2022). *Communication, Disinformation, Internet and Development*. First Annual International Conference on Religion, Culture, Peace, and Education. <https://www.academica.org/sergio.ricardo.quiroga/214> (accessed: 10.03.2024).
- Richmond Newspapers, Inc. v. Virginia* (448 U.S. 555) (1980). US Supreme Court. <https://supreme.justia.com/cases/federal/us/448/555/> (accessed: 10.03.2024).
- Rodrick S. (2014). "Achieving the aims of open justice? The relationship between the courts, the media and the public". *Deakin Law Review*, 19 (1), pp. 123–162. <https://doi.org/10.21153/dlr2014vol19no1art210>.
- Toriz Ramos C. (2021). "The Internet as Public Space: A Challenge to Democracies". In: A. Vizzizi, M.D. Lytras, N.R. Aljohani (eds.). *Research and Innovation Forum 2020: Disruptive Technologies in Times of Change* (pp. 555–563). New York: Springer International Publishing. <https://doi.org/10.1007/978-3-030-62066-0>.
- UNESCO (ed.) (2011). *Freedom of Connection – Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet*. United Nations Educational Scientific and Cultural.
- Venice Commission (2014). *Emerging Challenges to the Right to Privacy*. Council of Europe. [https://www.venice.coe.int/webforms/documents/?pdf=CDL-JU\(2014\)014-e](https://www.venice.coe.int/webforms/documents/?pdf=CDL-JU(2014)014-e) (accessed: 10.03.2024).
- Wagner A.J. (2022). "Whose Public Virtue? Exploring Freedom of Information Efficacy and Support". *Administration & Society*, 00953997221113223. <https://doi.org/10.1177/00953997221113223>.
- Wieshofer M. (2022). *Data Privacy Is Not Meta: Why Facebook's Foray Into the Metaverse Could Be Flawed From the Start*. <https://larc.cardozo.yu.edu/ciclr-online/36> (accessed: 10.03.2024).
- Zelezny J. (2010). *Communications Law: Liberties, Restraints, and the Modern Media* (Sixth edition). Boston: Wadsworth. <https://www.alibris.com/Communications-Law-Liberties-Restraints-and-the-Modern-Media-John-D-Zelezny/book/29583591?qsort=dr> (accessed: 10.03.2024).