UDK: 343.3/.7:004(450)

THE METAVERSE: ISSUES REALTNG TO CRIMINAL LAW

Federica di Simone
Researcher in Criminal Law, Università degli Studi della Campania Luigi Vanvitelli.
federica.desimone@unicampania.it

Abstract

There is yet no unanimity on the possible positive and negative developments and impacts that metaverse technology may have on humankind, but there is a clear need for the rapid adoption of a shared regulation capable of preventing the risks of harm to fundamental rights and ensuring the protection of rights in general. The legal questions that arise are not insignificant, and they also affect criminal science, regarding the resilience of both fundamental principles and the institutes proper to criminal law like the place where the offense was committed. The basic question is whether the tools offered by law today can be considered sufficient for the purpose of regulating the metaverse and the necessary protections, or whether the introduction of a specific discipline, capable of going beyond the traditional categories in favor of a law of the digital, is indispensable. The proposal of the creation of an electronic jurisdiction directed to the regulation of public relations taking place in the electronic, digital and virtual dimension, of which the metaverse is the most direct example of the cosmopolitan development of humanity, seems to be shareable. Through it, a kind of world citizenship could be achieved, in which electronic persons will acquire status and rights, while human persons will lose some of the rights proper to natural law and positive law and acquire new ones.

Keywords: *Metaverse, Criminal law, fundamental rights, legislation*, *space*

1. New scenarios

Smartphones, high-speed connections, social networks, digital payments and virtual currencies, biometric systems, quantum computers and artificial intelligence; these are only a few of the innovations that might lead us to consider the technological advances of the last fifty years as being without precedent, and among those with the greatest impact in human history. Relatively speaking, inventions such as fire, the wheel and printing – to name just a few – have had equally disruptive effects, but unique to modern times is the swiftness with which such innovations have been achieved, as well as the sheer quantity of discoveries that have been made almost simultaneously, and the speed with which these have been implemented in people's daily lives.[140]

Common to all periods, on the other hand, is the capacity to imagine the future through science fiction narratives, which have represented future scenarios that would later become reality.[141] Such is the

[140] There is no unanimity of views on the topic of technological development in anthropology and sociology, but the reconstruction of Ian McNeil, who has identified seven technological ages of humanity, stands out above all others. For further discussion, see I. MCNEIL, *An Encyclopedia of the History of Technology*, Londra, Routledge, 1990.

[141] Although the term science fiction was first used in 1926, man has been telling tales of fantastic and futuristic worlds since the dawn of time. We need only think of the novel *True History* of Lucian of Samosata, a writer who lived in the second century A.D., who told of landings on the moon, and of Philosopher Bacon's work, *The New Atlantis*,

case with virtual reality and augmented reality, parallel universes in which an alternative digital world is built to be experienced through the guise of an avatar, a concept that had been brought to life in both literature and film as early as the end of the twentieth century.[142]

The metaverse did not appear in our lives out of nowhere, but is rather the result of an idea that people had already conceived and partially realized over recent decades, albeit in rather rudimentary form.[143] Although there are various views on the possible development and impact that this technology may be capable of achieving, it is widely believed that there is an urgent need to adopt shared regulations capable of preventing violations of fundamental rights and ensuring, more generally, adequate protection of rights.

The European Union (EU), addressing this need, recently adopted the Digital Service Package, consisting of the Digital Service Act (DSA),[144] which focuses on the creation of a safe digital space for users and businesses, and the Digital Markets Act (DMA),[145] which aims to ensure a level playing field for all digital companies. This new legislation will also cover the metaverse, as a digital platform, as a space shared by users, and possibly as a virtual marketplace, pending ad hoc legislation due to be announced by the end of 2023.[146] The EU's objectives were explained by Thierry Breton, Commissioner for the Internal Market, who said, "this new virtual environment must include European values right from the beginning. People have to feel as safe in the virtual world as they do in the real world".[147]

The legal issues raised by the metaverse are considerable; it also creates problems for Italian criminal law, though here legal experts seem to approach the relationship between new technologies and general principles, on one hand, and the relationship between new technologies, criminal cases and the administration of justice, on the other, separately and at different speeds.[148] Investigation of the

written in 1624 and anticipating some technological discoveries of our own day. See https://www.ilsole24ore.com/art/storia-vera-luciano-e-nasa-ADtfXDn e P. ROSSI (a cura di), *La Nuova Atlantide e altri scritti*, in *Scritti filosofici*, Torino, Utet, 2009, pp. 1975-2016.

[142] Something similar to the Metaverse, in fact, was imagined as early as the late 1990s in the famous film *Matrix* and in 2010 by writer Ernest Cline in his cyber thriller *Ready Player One*, of which a film adaptation directed by Spielberg was curated in 2018.

[143] *Second life* and *MySpace* platforms anticipated the virtual world of the Metaverse in the early 2000s, but perhaps the time was not ripe for such an innovation, and they were not followed up over time.

[144] EU Regulation 2022/2065 del 19 ottobre 2022, in *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022R2065&from=EN*.

[145] EU Regulation 2022/1925 del 14 settembre 2022, in *https://eur-lex.europa.eu/legal-content/IT/TXT/PDF/?uri=CELEX:32022R1925&from=EN*.

[146] Parliamentary Question E-000656/2022 was devoted to the Metaverse, with the dual request to initiate a study about its operation and potential risks to citizens, and to adopt specific regulations. See *https://www.europarl.europa.eu/doceo/document/E-9-2022-000656_IT.html*. If, initially, the European Commission had responded negatively, deeming sufficient a monitoring of the new platform and the concomitant application of the new regulatory instruments, an unexpected and sudden revirement led to the letter of intent by which the Commission itself counted among the key initiatives for 2023 that on virtual worlds such as the Metaverse. See *https://www.key4biz.it/wp-content/uploads/2022/09/SOTEU_2022_Letter_of_Intent_EN_0.pdf*.

[147] *https://www.agendadigitale.eu/cultura-digitale/il-metaverso-questo-sconosciuto-ecco-perche-e-impensabile-normarlo-ora/*.

[148] Criminal law's interest in new technologies is witnessed especially at the supranational level. See, for example, the adoption of specific regulations, such as the European Parliament Resolution of October 6, 2021, entitled *Artificial Intelligence in Criminal Law and its Use by Law Enforcement and Judicial Authorities in Criminal Law*. On the front of doctrinal reflections on general principles and new technologies, contributions are not yet very numerous. C. CUPELLO, *La sfida dell'intelligenza artificiale al diritto penale*, in *https://www.sistemapenale.it/it/scheda/cupelli-la-sfida-dellintelligenza-artificiale-al-diritto-penale*, 21 aprile 2023; F. BASILE, *Intelligenza artificiale e diritto penale: qualche aggiornamento e qualche nuova riflessione*, in G. BALBI, F. DE SIMONE, A. ESPOSITO, S. MANACORDA (a cura di), *Diritto penale e intelligenza artificiale. Nuovi scenari*, Torino, Giappichelli, 2022; C. PIERGALLINI, *Intelligenza artificiale: da 'mezzo' ad 'autore' del reato?*, in Riv. It., Dir. Proc. Pen., 2020; S. RIONDATO, *Robot: talune implicazioni di diritto penale*, in P. MORO, C. SARRA (a cura di), *Tecnodiritto,* Milano,

compatibility of new legal instruments with the principles of the existing system does not yet seem to be central to the debate, while the proliferation of instruments in the field at an international level has encouraged legislators to intervene, defining new offences and modifying those that already exist, in an attempt to curb the expansion of cybercrime. This increase in international instruments has also inspired doctrinal development in a number of ways.

Compared to the bases of criminal law, the principles of materiality and offensiveness seem to suffer in particular when put in relation to new technologies, and this is all the more evident in the virtual realm. At a global level, there is still no solution for the problem of determining responsibility for acts committed by artificial intelligence systems, an issue which, within our legal order, could constitute a point of friction both with the principle of guilt, and even before that, with the culpability principle, as specified in Article 27 para. 1 of the Constitution.[149] Transposed into the metaverse, the issue exists in analogous terms for the virtual world too, both in cases in which an avatar takes the guise of an active subject, and those in which an avatar is itself victim of a crime. Before dealing with the problem of which regulation is applicable – i.e., whether one should apply that envisaged for legal entities by Legislative Decree no. 231/2001, as suggested by parts of the doctrine,[150] whether it would be more appropriate to make use of the theory of representation or regulation envisaged for assigning responsibility in the case of damage caused by animals, or whether the best solution would be to introduce some autonomous form of electronic personality[151] – certain technical questions need to be examined.

At the moment only human beings may possess an avatar in the metaverse; however, recent experiments suggest that artificial intelligence will soon also have its own avatars, and this greatly complicates things in terms of determining criminal responsibility, since there is not yet any agreement on

---

Franco Angeli, 2020; V. MANES, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in U. RUFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, Giuffrè, 2020, pp. 547 ss.; L. PICOTTI, *Diritto penale e tecnologie informatiche: una visione di insieme*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), *Cybercrime*, Milano, Utet, 2019, pp. 35 ss.; C. BURCHARD, *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società*, in Riv. It. Dir. Proc. Pen., 2019, 62, 4, pp. 1909 ss. In tema di fattispecie penali, nuove tecnologie e giustizia, *ex multis* F. DE SIMONE, *L'implementazione delle nuove tecnologie nelle politiche anticorruzione*, in, in G. BALBI, F. DE SIMONE, A. ESPOSITO, S. MANACORDA (a cura di), *Diritto*, cit.; F. BOTTALICO, *Il furto di identità digitale*, in G. SICIGNANO, A. DI MAIO (a cura di), *Nuove problematiche in tema di reati informatici*, Milano, La Tribuna, 2022, pp. L. DELLA RAGIONE, *Il delitto di frode informatica: l'art. 640 ter c.p.*, in G. SICIGNANO, A. DI MAIO (a cura di), *Nuove problematiche*, cit., pp. 61 ss.; F. DE SIMONE, *I delitti contro l'integrità dei dati dei programmi e dei sistemi informatici: gli attacchi "Denial of Service*, in G. SICIGNANO, A. DI MAIO (a cura di), *Nuove problematiche*, cit., pp. 43 ss.; A. ESPOSITO, *Il cyberbullismo*, in G. SICIGNANO, A. DI MAIO (a cura di), *Nuove problematiche*, pp. 143 ss.; G. GENTILE, *Il furto di dati informatici*, in G. SICIGNANO, A. DI MAIO (a cura di), *Nuove problematiche*, cit., pp. 89 ss.; R. GIORDANO, A. PANZAROLA, A. POLICE, S. PREZIOSI, M. PROTO (a cura di), *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia*, Milano, Giuffrè, 2022; M. CROCE, *Cyberlaundering e valute virtuali. La lotta al riciclaggio nell'era della distribuited economoy*, in Sist. pen., n. 4, 2021, 129 e ss.; M. GIUCA, *Criptovalute e diritto penale nella prevenzione e repressione del riciclaggio*, in Dir. pen. cont. riv. trim., 2021; T. PIETRELLA, *Reati informatici e concorso di norme: come l'evoluzione tecnologica informa il diritto penale. Il caso delle botnets*, in Discrimen 2 dicembre 2021; E. RIVA, *Le fattispecie di danneggiamento informatico: una comparazione tra Italia e Cina*, in Sistema pen., 2021, 4, pp. 105 ss; O. DI GIOVINE, *Il "judge-bot" e le sequenze giuridiche in materia penale (intelligenza artificiale e stabilizzazione giurisprudenziale)*, in Cass. Pen., 2020, pp. 952 e ss.; M. CATERINI, *Il giudice penale robot*, in La legisl. Pen., 19.12.2020; M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa*, ivi, 29 maggio 2019.

[149] A. CAPPELLINI, *Machina delinquere non potest. Brevi appunti su intelligenza artificiale e responsabilità penale*, in Criminalia, 2018, pp. 499 ss.

[150] D. INGARRICA, *Metaverso criminale. Quali interazioni nel presente nazionale e quali sfide globali del prossimo futuro*, in Giur. Pen. Web, 2022, 9, pp. 8 ss.

[151] S. CHESTERMAN, *Artificial Intelligence and the problem of Autonomy*, 2019, in Journal on Emerging Technologies, 2020, 1, 2, pp. 222 ss.

who ought to be responsible for the conduct of artificial intelligence in general. Two possibilities, which are far from remote, have not been taken into account. The first is that it will be impossible to tell apart an avatar controlled by a person from one controlled by artificial intelligence.[152] The second is that within the metaverse one may act anonymously, and it may not be possible to trace personal data and track down the owner of an avatar, given that even blockchain technology does not provide absolute guarantees of inviolability.[153]

If we consider instead the relationship between new technologies and criminal cases, criminal law has already been facing up to digital criminality[154] and the virtual realm for some time: 1993, for instance, saw the introduction of the crime of illegal access to a digital or computerized system (Art. 615 *ter* of the Criminal Code), de facto making a digital address equivalent to a physical address; while 2006 saw the introduction of the crime of virtual pedophilic pornography (Art. 600 *quater*).[155]

Circumstances make it necessary to regulate cases that may occur in the metaverse, whether through ad hoc regulations or through the extensive interpretation of cases that have already been foreseen. Already, the case history includes a complaint filed by a researcher in regard to sexual violence inflicted by other avatars against her avatar during tests carried out in virtual reality.[156] Sexual violence,[157] it is true, is one of the more difficult cases to transpose into the virtual realm: on the basis of the text of the case, the typical elements of such crimes can immediately be excluded even in abstract, given the absence of physicality in the virtual world, and thus the lack of typical materiality. However, it is also true that continuing manipulation of normative requirements by scholars and practitioners of jurisprudence has already led the Court of Cassation to recognize grounds for sexual violence in the absence of physical contact through an act carried out via chat.[158]

---

[152] S. ATERNO, *Profili penali della vita nel metaverso*, in G. CASSANO, G. SCORZA (a cura di), *Metaverso. Diritti degli utenti – piattaforme digitali – privacy – diritto d'autore – profili penali – blockchian e NTF*, Pisa, Pacini Giuridica, 2023, p. 427.

[153] F. SARZANA DI SANT'IPPOLITO, M.G. PIERRO, I.O. EPICOCO, *Il Diritto del Metaverso. NFT, DeFi, GameFi e privacy*, Torino, Giappichelli, pp. 79 ss.

[154] So-called *cybercrimes* do not fit into a legally defined category. On this point see R. FLOR, *La legge penale nello spazio, fra evoluzione tecnologica e difficoltà applicative*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Cybercrime*, cit., p. 151 e L. PICOTTI, *La nozione di criminalità informatica e la sua rilevanza per le competenze penali europee*, in Riv. Trim. dir. Pen. economia, 2011, 4, pp. 827 ss.

[155] A body of rules, codified and extra-codified, have over time been introduced into the legal system to regulate various hypotheses of computer crimes. Suffice it to think of the cases of abusive access and violation of computer systems, the hypotheses of destruction and damage of the same, as well as the cases of computer fraud or the spread of viruses. The listing has only an illustrative value and reference is made to the reference bibliography, as this is not the place for an in-depth study of the subject. L. PICOTTI, *Cybercrime und strafrecht digitalisierung, globalisierung und risikopravention. festschrift fuer ulrich sieber zum 70. geburtstag*, Berlino, Duncker & Humblot, 2021, pp. 807-830; L. PICOTTI, *Cybercrime e diritto penale*, in C. PARODI, V. SELLAROLI (a cura di), *Diritto penale dell'informatica. Reati della rete e sulla rete*, Milano, Giuffrè, 2020, pp. 709-723; A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Cybercrime*, cit.

[156] To prevent such cases, the platform operator has introduced the possibility for avatars who feel threatened to resort to a safe zone. On this point, see A. CONTINIELLO, *Le nuove frontiere del diritto penale nel Metaverso. Elucubrazioni metagiuridiche o problematica reale?*, in Giur. Pen. Web, 2022, 5, pp. 1 e ss. In generale v. G. ALESCI, *Meta - reato tra presente e futuro: alcune riflessioni critiche*, in V. NUZZO, M. RUBINO DE RITIS, A. FUCCILLO (a cura di), *Diritto e Metavserso*, Napoli 2023.

[157] G. BALBI, *I reati contro la libertà e l'autodeterminazione sessuale in una prospettiva di riforma*, in Sist. Pen., 3 marzo 2020. Si veda anche S.R. PALUMBIERI, *I delitti contro la libertà sessuale* (voce), in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), *Diritto Penale*, Milano, Utet, 2022, pp. 6171 ss.

[158] On whether or not there needs to be physical contact to integrate the extremes of sexual assault, in a case of allusive message exchanges by means of a chat room, see Cass., Sez. III, 8 September 2020 n. 25266, according to which the undue interference in the sexual sphere of the passive subject taken into consideration by Article 609-bis of the Criminal Code is integrated even in the absence of physical contact, whenever the sexual acts involve the corporeality

The metaverse may also be the setting for crimes carried out against public administration. Given that some public authorities have announced their intention to set up consultation booths within the metaverse, it is not abstract speculation to consider, for example, the possibilities for instances of corruption, whether public or private.[159]

Beyond profiles of typicality and, more generally, of criminal liability, there is another important aspect that must be approached: how one ought to identify the place in which an act is to be considered to have occurred within the metaverse, if it is held to be a crime. The present article will focus on the so-called *locus commissi delicti* in this regard.

It would be inappropriate here to discuss the definition and essence of space within the metaverse. From a philosophical perspective, this may exemplify one of the heterotopic spaces theorized by Foucault, insofar as it is a place that is the outcome of connections between those spaces in which one sees a suspension, if not an outright neutralization, of the human relationships that they reflect, in the same way as a mirror, a cemetery, or a prison.[160] Another way to read the metaverse would be to take an anthropological approach, and see it as a place without identity constructed for a specific end, similarly to means of transport, or to leisure zones.[161]

More concretely, for users of the web in general, and for users of the metaverse in particular, the importance of spatial-temporal coordinates is greatly reduced, since what predominates in the latter case is the immersive aspect *tout court*.[162]

Law, on the other hand, grasps the requirements of regulation, and is duly incorporating the technical explanations of the hard sciences and the widely shared definition given by Michel Ball in his famous book, *Metaverse*.[163] For criminal law in particular, it is fundamentally important to understand precisely what kind of place the metaverse is and identify its boundaries in a traditional sense. This will determine the identification of applicable national laws, and consequently the identification of suitable jurisdiction.

2. The cross-border dimension of the metaverse

The particular structure of the metaverse and the unimportance of geographic boundaries in relation to the way certain types of crime function require us to think about the issue of transnationalism and the possibility of using shared international parameters that deal specifically with virtual reality, rather than

---

of the offended person and are aimed at and suitable for compromising the primary good of individual freedom with a view to satisfying or arousing one's sexual instincts.

[159] Some public administrations, such as the Piedmont Region, have shown their intention to open public offices in the Metaverse. In particular, the Piedmont Information Systems Consortium and some health care companies are investing resources to take advantage of its potential, offering the possibility of accessing public services such as the payment of stamps and co-payments. See Some public administrations, such as the Piedmont Region, have shown their intention to open public offices in the Metaverse. In particular, the Piedmont Information Systems Consortium and some health care companies are investing resources to take advantage of its potential, offering the possibility of accessing public services such as the payment of stamps and co-payments.

[160] M. FOUCAULT, *Spazi altri. I luoghi delle eterotopie*, Vaccaro S. (a cura di), Milano, Mimesis, 2001.

[161] M. AUGÉ, *Non luoghi. Introduzione a una antropologia della surmodernità*, D. ROLLAND, C. MILANI (Traduzione a cura di), Milano, Eleuthera, 2009.

[162] G. PICA, *I reati nella società dell'informazione*, in S. ALEO, G. PICA, *Diritto penale. Parte Speciale II*, Padova, Cedam, 2012, pp. 1015 ss.

[163] M. BALL, *Metaverso. Cosa significa, chi lo controllerà e perché sta rivoluzionando le nostre vite*, G. MANCUSO (Traduzione a cura di), Milano, Garzanti, 2022. According to the author, *the metaverse is a massive, interoperable network of 3d virtual worlds with real-time rendering that can be experienced synchronously and persistently by an effectively unlimited number of users with a sense of individual presence and with continuity of data such as identity, history, rights, objects, communications and payments*.

general regulations and the principles contained in individual pieces of legislation, which in any case have not been brought into harmony.[164]

The complexity of the issue has already been made plain when legislating against cybercrime, whose crosss-border nature was immediately clear, and in respect of which the Convention on Cybercrime was adopted in 2001.[165] Although this contains a provision regarding the possibility of "trans-border access to stored computer data with consent or where publicly available" (Art. 32), the document does not define the concept of trans-border access and limits itself to giving a few criteria for establishing State jurisdiction (Art. 22).[166]

We may derive a definition of transnational crime from the punitive measures motivated by the need to repress common cases, in which the criminal act crosses State borders even only in part, or has effects in various countries.

This was the case for offences associated with organized crime, for which the United Nations Convention signed in Palermo in 2000 lists, in Article 3, the criteria for which States may consider a crime to be transnational in nature. The Convention provides a definition of transnational crime that, though it refers specifically to organized crime, may also be applied generally. Article 3, paragraph 2 affirms that a crime is transnational if: a) it is committed in more than one State; b) it is committed in one State but a substantial part of its preparation, planning, direction or control takes place in another State; c) it is committed in one State but involves an organized criminal group that engages in criminal activities in more than one State; or d) it is committed in one State but has substantial effects in another State.

Given all this, cybercrimes are *in re ipsa* transnational in the majority of cases, and that will most likely also be true for crimes committed in the metaverse, given the ubiquitous character of the connections on which these systems are based. One might find, for example, that the registered office of a given platform and the digital systems on which its virtual reality depends are located in a different State from that in which the perpetrator of a crime or its victim reside; however, it may also happen that a crime is initiated in the real world and concluded in the virtual world, or vice versa. Consider, for instance, what may happen in the case of an established criminal organization, which could use the metaverse as a place in which to organize crimes that could then be carried out in either the real or virtual world.

These specificities clearly result in a need for ad hoc regulations for potential cases that take into account the transnational character of the virtual world, given the obvious effects that may arise from the difficulty of precisely identifying the *locus commissi delicti*, as well as the risks of violating general principles such as *ne bis in idem*. The Palermo Convention imposes obligations on States to make alterations to their own legislation, which Italy already respects, however, given existing national legislation on the matter.

Recognition of the transnational character of the metaverse, if it is also to have a concrete effect in terms of international cooperation, would however require that each State identifies, or defines, the specific criminal situations on the basis of which it can prosecute acts committed in this setting.

3. Spatial coordinates according to Italian criminal law

To approach the issue of *locus commissi delicti* in regard to the metaverse, we may, in my opinion, follow two different lines of inquiry.

The first sees the virtual environment as being different and supplementary to the real world, but nonetheless a place in which activities may be undertaken that are similar to those that exist in the real world, among them the perpetration of crimes. This makes the extension into the metaverse of existing

[164] A. DI MARTINO, *La frontiera e il diritto penale, Natura e contesto delle norme di "diritto penale transnazionale"*, Torino, Giappichelli, 2006.

[165] In *https://www.coe.int/web/cybercrime/home*.

[166] R. FLOR, *Cyber-criminality: le fonti internazionali ed europee*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA, *Cybercrime,* cit., pp. 97 ss.; L. PICOTTI, *La ratifica della Convenzione Cybercrime del Consiglio d'Europa. Profili di diritto sostanziale*, in Dir. Pen. e processo, 2008, 6, pp. 700 ss.

regulatory criteria in criminal codes both credible and logical, though given the peculiarities of this new space some of these criteria will be more applicable than others.

The second, on the other hand, does not admit the spatial nature of the metaverse, and instead opts for a despatialized reconstruction of the concept, which would require specific regulations quite different from those that already exist.

I believe this latter approach is preferable for two reasons. The first is the need to introduce a system of criminal justice tailored to the regulatory needs of a setting for which it seems unsatisfactory simply to refashion regulations conceived at a time when the phenomenon in question was unknown. Second, this choice may also solve issues which, in relation to certain cases, already make regulation difficult in space understood in the traditional sense; the peculiar character of the metaverse would only provide further complications.

By this I refer, for instance, to the problems of effectively protecting assets with widespread ownership, and of instances in which the victim of the crime is unspecified.[167]

Nonetheless, as things stand – whether one decides to view the metaverse as a "place", albeit one with extremely peculiar characteristics, or instead consider it as a "non-place" or heterotopia – I believe that it is simpler, in the near term, to regulate virtual space alongside physical and digital space according to the rules in force, adding corrective measures as indicated in recent years by jurisprudential practitioners.

As early as 1930 Italian criminal legislators saw the concept of space as being untethered from geographical and national boundaries, to the extent that the Italian Criminal Code, in some people's view, embraces a principle of moderate territoriality,[168] while others see it as expressing a tendency to adhere to the principle of universality,[169] or in any case as being characterized by a marked extension of the criteria that provide a basis on which to establish Italian jurisdiction, even if the crime is committed abroad. According to the latter perspective, the dynamics of attribution are further unbalanced by acceptance of the principle of ubiquity, which establishes parameters for identifying the *locus commissi delicti* in a way that allows an enormous number of crimes to be considered as being committed on Italian territory, even when these are largely carried out abroad.

Under the conditions set forth by Articles 7, 8, 9 and 10 of the Criminal Code, Italian law is already enforceable well beyond the national borders.

The criteria used by the Criminal Code are able to define the space of the metaverse, helping to resolve the interpretative uncertainty regarding the *locus commissi delicti*, both at the electronic and digital level, and in the virtual realm.

The principle of ubiquity has two criteria that can be used to identify it: one may consider the place in which the criminal act or omission occurred, whether in whole or in part, or one may make reference to the place in which the event constituting the result of a criminal act or omission occurred.

As regards crimes committed in the metaverse, the lack of materiality means that one cannot physically locate the offender's conduct in physically identified territory, and, similarly, one cannot determine the place in which the effects of the crime have occurred. However, avatars, even in their capacity as "perpetrators" and "victims" of crime, are not subject to law – or at least, are not so yet. The debate accordingly shifts to their owners, creating a sort of *fictio iuris* and thus returning to a spatially well-defined area. Will it therefore be necessary to consider the place in which the owner of the avatar who has perpetrated a criminal act is located, or the place in which the owner of the avatar victim of a criminal act is located, even though the act or omission has occurred elsewhere?

In fact, even these parameters do not offer a valid solution to the problem, and indeed the jurisprudence for the case of illegal access to a digital system pursuant to Article 615 *ter* of the Criminal

---

[167] F. CAMPLANI, *Locus commissi delicti, norme di collegamento e reati informatici a soggetto passivo indeterminato*, in Arch. Pen., 2020, 2, pp. 9 ss.

[168] G. FIANDACA, G. LEINERI, *Sub art. 6 c.p.*, in FORTI G., SEMINARA S., ZUCCALÀ G., *Commentario breve al codice penale*, Milano, Cedam, 2017, pp. 36 ss.

[169] G. MARINUCCI, E. DOLCINI, G.L. GATTA, *Manuale di diritto penale, Parte generale*, Milano, Giuffrè, 2020, p.p. 136 ss.

Code has highlighted its limits. Rejecting the guidelines that at times situate the *locus commissi delicti* in the place in which the server is located, at other times in the place in which the subject agent is located, the Court of Cassation affirms that "access begins only with human action of a material nature, consisting in the user typing authentication credentials remotely, while all subsequent events are to be understood as communicative behavior between the client and the server.

"Unauthorized access or introduction, then, is completed in the place in which the operator physically types an access password and follows the login procedure, whose effect is to overcome the security measures set up by the system owner, thus achieving access to a database. From this approach, which is consistent with how an electronic network actually works, it follows that the location in which the crime is committed is that in which the agent interfaces remotely with the entire system, entering authentication credentials and clicking 'Start', thus implementing the only material and voluntary action that puts him/her in a position to enter the information domain that is viewed directly from within the remote location."[170]

Couched in such sensible language, this criterion, which I would define as that of "input",[171] may seem definitive for possible cases in the Metaverse as well – except that the offender might well make use of the numerous options afforded by the technology to cloak his/her location, or, more simply, might connect using someone else's device. The only thing to do, in consequence, is to refer to the regulation indicated as an alternative by the provisions of Article 6 of the Criminal Code, and consider the place in which the effects of the crime occur, which, since this cannot be the Metaverse itself, should coincide with the location of the victim. However, it may happen that even in such cases the identification of the *locus commissi delicti* may not immediately be clear, since, for instance, there could be several victims, not all of whom are connected to the platform at the moment the crime is committed, or the effects of the crime may occur some time after the computer command is received. It follows that the two parameters identified in the Criminal Code may not be applicable in some cases, leaving the issue open, as happens when we use them for crimes of opinion and online defamation cases.

It therefore seems worthwhile to analyze the solution adopted in jurisprudence regarding legitimacy in the field of online defamation, in the case of an offence committed by a citizen through a foreign site, when this affects one or more subjects located in national territory. In 2008 the Court held that "in such cases Italian judges are authorized to determine the defamation carried out by posting offensive phrases and/or defamatory images on the computer network (Internet), even in cases in which the website is registered abroad, provided that the offence affects several users who are located in Italy; insofar as it an offence involving an event, defamation occurs at the moment and place in which third parties experience the offensive expression".[172]

In such cases one may apply what, in my opinion, could be called the "criterion of perception", for which it is necessary to consider the place in which the offence is experienced, which does not necessarily coincide with the place in which the victim was found at the moment the crime was committed. Nor should we underestimate the potential of this parameter with regard to the issue of a pre-established natural judge, wherever cyberspace lends itself to potential cases in which the subject agent pre-programs the phases of a crime's consummation in such a way as to evade jurisdiction.

---

[170] Cass, Sez. Un., 24 aprile 2015 n. 17325; Cass., Sez. V, 21 luglio 2015 n. 31677. R. FLOR, *I limiti del principio di territorialità nel "cyberspace". Rilievi critici alla luce del recente orientamento delle sezioni unite*, in Dir. Pen. processo, 2015, 10, pp. 1296 ss.

[171] The writer takes her cue for the definition of the criterion under consideration from the appellation 'immiss' (from the Latin immitto, immittis, to introduce) originally given to the enter key inserted on computer keyboards and which only later came to be known as 'enter.' W. MARASCHINI, C. SCAGLIARINI, *Algoritmi in Pascal*, Torino, Paravia ed., 1995, pp. 3 ss.

[172] Cass., Sez. II, 25 settembre 2008 n. 36721. Before, Cass., Sez. V, 21 giugno 2006 n. 25875, according to which defamation, as an event crime, is consummated at the time and place when third parties perceive the insulting expression. R. FLOR, *La legge*, cit., pp. 155 ss.

This parameter was further confirmed by the Court of Cassation itself in subsequent pronouncements regarding similar cases, with the judges arguing that the location to be considered is that in which one receives the digital information through which a crime is committed.[173] German jurisprudence had previously reached an analogous solution for an even more complex case regarding the crime of "mass incitement". Specifically, the offence was carried out on foreign territory by a German citizen who spread Holocaust-denying material on a website registered in Germany, a situation further complicated by the fact that the laws of the State in which the act was committed did not consider this to be a criminal offence, unlike in Germany. In this case too, judges applied the "criterion of perception", arguing that one should apply legislation from the country in which the offence would be experienced and have an effect.[174]

A solution of this sort may find wide application especially in the near future, when one will be able to access the metaverse solely via a virtual reality (VR) headset, in those cases in which the device is used from abroad. In the case of augmented reality, the distance between real space and virtual space will be almost completely removed, along with the perception of otherness between an individual and his/her avatar.[175] This will be another problematic area when it comes to identifying the place in which a crime is committed, which could be resolved by determining the place in which the offence is experienced by the victim; an across-the-board solution, this, both for conceptions of the metaverse as a secondary and different instance of space, and as a non-space.[176]

As is well known, following Article 7 of the Criminal Code, Italian criminal law has unconditional application for certain cases, such as crimes against the personality of the Italian State and crimes committed by public officials in service of the State, should they abuse their powers or violate the duties inherent to their roles, whether these are committed by Italian citizens or foreigners, in foreign territory. We need to consider the possibility that such crimes may be committed in the metaverse, and reflect on the appropriate penal measures.

The solution appears to depend on how one conceives of virtual space. If one wanted to recognize the metaverse as a "place", one might consider the main office of the company that controls the platform, or the location of its servers; one might also make use of the criterion of input. As regards the criterion of perception of the offence, on the other hand, this accords less well with the bases of the regulations in question, insofar as the extension of Italian jurisdiction is justified by the gravity of the crimes being considered, and by the public nature of the assets affected by the crime, which from a logical and hermeneutical perspective push issues related to the perception of the offence into the background. Furthermore, from a practical point of view, the importance of the issue is reduced by the fact that these are crimes that can be punished regardless of the place in which they are committed.

4. Public and private spaces in the metaverse

Legislation for some offences requires that the act be carried out in public places or places open to the public, as in the case of harassment or disturbance of persons provided for by Article 660 of the Criminal Code, or that of obscene acts, as per Article 527 of the Criminal Code. Both cases might well occur in the metaverse environment, and accordingly there arises the question of how this space should be understood.

As regards the distinction between a public place and a place open to the public, a recent ruling of legitimacy,[177] positioning itself in continuity to the United Sections of 2019,[178] restated that a public place means an open space that people may use freely, in which anyone may pass through and/or stay without

[173] Cass., Sez. I, 26 gennaio 2011 n. 2739; Cass., Sez. I, 26 aprile 2011 n. 16307; Cass., Sez. V, 21 luglio 2015 n. 31677.
[174] F. CAMPLANI, *Locus*, cit., pp. 19 ss.
[175] E. DINCELLI, A. YAYLA, *Immersive virtual reality in the age of the Metaverse: A hybrid-narrative review based on the technology affordance perspective*, in The Journal of Strategic Information System, 2022, 31, 2.
[176] S. ATERNO, *Profili*, cit., p. 424.
[177] Cass., Sez. I, 16 febbraio 2021 n. 6089.
[178] Cass., Sez. Un., 28 marzo 2019 n. 46595.

requiring any particular permission. Meanwhile, a place open to the public may be used by anyone, without distinction, provided they have whatever authorization may be required, or a ticket bought upon entrance. A place is private, on the other hand, when access is given only to a determined number of people who are identified by name.[179]

A 2014 ruling on the applicability of Article 660 of the Criminal Code in cases of harassment carried out over the internet and through social networks avoided the problem of whether digital communications were to be treated as equivalent to telephonic communications. Rather, to admit behavior on platforms such as Facebook as possible cases of harassment or disturbance of persons it would be necessary to assimilate digital space within physical space and consider the former as a place available for any Web user to access. According to the Court of Cassation, "it seems impossible to deny that the social network Facebook is a sort of virtual agora, an 'immaterial public square' that allows an indeterminate number of 'accesses' and views, enabled by technological evolution, which legislators certainly had never imagined. And yet the letter of the law does not exclude it from being considered as a place; given the revolution that has been brought about in regard to forms of social gathering and traditional notions of community, its rationale in fact makes this view obligatory."[180]

For the purposes of this decision the question of whether a social network is a public place or a place open to the public is not a nullifying one; indeed, the Court makes no distinction in this regard, preferring to emphasize the social network's nature as an open place. In my view, however, it seems clear that Facebook falls within the second category, since only registered users may access the platform.

The same goes for the virtual world. Whether one take a centralized metaverse managed by a single entity (as in the case of Meta), or a decentralized platform administered by various managers (as in the case of Decentraland), users cannot access these freely, as is usually done on the Web, but must first register. This means that the metaverse is a place open to the public, with all associated consequences: the open and common zones in which avatars meet cannot be considered public spaces.

On closer inspection, though, unlike social networks, in the metaverse, alongside spaces that are open to the public, we can also identify private spaces. One may buy virtual locations in which, for example, one can carry out one's business, as has recently happened with an Italian law firm, which aims to use the space it has purchased in the metaverse as a virtual headquarters for its legal consultancy business, or various medical clinics which plan to do something similar for virtual consultations. In these cases we would be dealing with private space, which can only be accessed by avatars who have been previously identified and who have perhaps arranged an appointment. As such, these would not fall under the rules applicable to public spaces, and consequently the applicability of certain crimes must be excluded – as well as the grounds for others.

5. On the threshold of *e-law*

The juridical regulation of new and emerging phenomena brings with it the risk of putting curbs on facilities that by their very nature are intended to be unrestricted. This conviction initially also applied to the Web, to the extent that "for decades, at every fork in the road we reached, between strictly regulating and not regulating the digital ecosystem that was growing and developing around the network we called the Internet, most of us suggested, without any hesitation, the road of deregulation. 'Technology is neutral', […], it is up to people to decide how to use it and find a way to orient it towards the maximization of the common good in the interests of the majority".[181] However, as we reach the threshold of a fifth industrial revolution, in which the real and biological worlds seamlessly coincide with the digital world, where people

[179] Cass., Sez. Un., 31 marzo 1951 n. 8.
[180] Cass., Sez. I, 12 settembre 2014 n. 37596.
[181] G. SCORZA, *In principio era Internet e lo immaginavamo diverso*, in Riv. It. Inform. Dir., 2022, 1, pp. 13 ss.

increasingly undergo an "onlife" experience,[182] scholars are ever more convinced of the need to regulate new technologies effectively.

Recent alarms[183] raised by various people about the risks that may be associated with the massive use of artificial intelligence systems make Rodotà's words ever more topical: he said that governing new discoveries means guaranteeing the rights and freedoms of all.[184] The European Union is well aware of this, and recently adopted its first law on artificial intelligence, better known as the AI Act, based on a risk assessment of the various artificial intelligence systems and aimed at establishing a uniform legal framework that will ensure the development, marketing and use of these systems complies with the values and constitutional rights of the EU.[185]

The metaverse also fits within this landscape of innovation, change, and fear, and constitutes an entity that is perhaps more complex than we are currently able to grasp. The founder of one metaverse system, Mark Zuckerberg, has described it thus: "Critically, no one company will run the metaverse – it will be an 'embodied internet', operated by many different players in a decentralized way."[186] A new form of the internet, in other words, literally "embodied", in which participants will not merely be passive viewers, but themselves be part of the experience – which means that crimes there may be committed just as they are in the real world. It will accordingly be necessary to ascertain to what extent the metaverse reproduces positive and negative aspects of real life, given that it will not be able to escape the attention of existing laws in the event that similarities become increasingly clear. This begins with digital identity, which may fall within the framework of Article 2 of the Italian Constitution to the same extent as personal identity.[187]

At root, the question is whether the tools made available by current laws can be considered sufficient for the regulation of the metaverse and as a means of providing necessary protection, or whether new, specifically designed legislation is necessary, capable of moving beyond traditional categories in favor of digital law, somewhat akin to what happened in the case of maritime law, once it had become clear that maritime space could not simply be assimilated within terrestrial space, and that the laws envisaged for the latter were inappropriate for the former. But while in the case of maritime law the question was made one of difference of space, digital processes have expanded to such an extent that spatial-temporal parameters have practically been cancelled out, while the possibility of acting remotely in a virtual world gives the lives we will lead in the near future a planetary dimension. Among the first things to collapse may be national and political boundaries, in which case a *locus commissi delicti*, like so many other things, will likely be relegated to another era.

---

[182] L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, Raffaello Cortina ed., 2017, according to which the boundaries between online and offline life tend to disappear and we are now seamlessly connected to one another, progressively becoming part of a global "infosphere." This epochal shift represents nothing less than a fourth revolution, following those of Copernicus, Darwin and Freud.

[183] Fears that virtual worlds may translate into dangerous places are not the preserve of the law alone. Recent studies in sociology and psychology, in fact, denounce the risks that could result from leading a parallel life in the Metaverse, including the weakening of interpersonal relationships, an increased tendency toward escapism and entertainment, and the danger that people will become less and less able to cope with reality. T. OLEKSY, A. WNUK, M. PISKORSKA, *Migration to the metaverse and its predictors: attachment to virtual places and metaverse-related threat, in Computers* in Human Behavior, 2022; M. MASTROGIOVANNI, *Intermedialità e rimediazione nel metaverso una ricognizione bibliografica ragionata (con qualche proposta)*, in Riv. Interd, Com., 2022, 4, pp. 96.

[184] S. RODOTÀ, *Tecnologie e diritti*, Bologna, Il Mulino, 2021.

[185] See *https://artificialintelligenceact.eu/*. The European Parliament had already expressed reservations about the use of such systems in criminal justice and, in this regard, passed the Resolution on Artificial Intelligence in Criminal Law and its Use by Law Enforcement and Judicial Authorities in 2021, in *https://www.europarl.europa.eu/doceo/document/TA-9-2021-0405_IT.pdf*.

[186] Thus, MARK ZUCKERBERG in a recent interview, in *https://www.theverge.com/22588022/mark-zuckerberg-facebook-ceo-metaverse-interview*.

[187] D. INGARRICA, *Metaverso*, cit., p. 6.

Given all this, we can commend the proposed creation of a digital jurisdiction aimed at regulating public relations that take place in the electronic, digital and virtual realm. The metaverse is the most direct example of these, as well as of humanity's cosmopolitan development. With the help of such digital jurisdiction, a sort of global citizenship might be achieved, in which digital people will acquire status and rights, while human people will lose some of those associated with natural law and positive law, but gain new ones[188] that can be asserted in a single new meta-place.

REFERENCES LIST

G. ALESCI, *Meta - reato tra presente e futuro: alcune riflessioni critiche*, in V. NUZZO, M. RUBINO DE RITIS, A. FUCCILLO (a cura di), *Diritto e Metaverso*, Napoli 2023; S. ATERNO, *Profili penali della vita nel metaverso*, in G. CASSANO, G. SCORZA (a cura di), *Metaverso. Diritti degli utenti – piattaforme digitali – privacy – diritto d'autore – profili penali – blockchian e NTF*, Pisa, Pacini Giuridica, 2023; M. AUGÉ, *Non luoghi. Introduzione a una antropologia della surmodernità*, D. ROLLAND, C. MILANI (Traduzione a cura di), Milano, Eleuthera, 2009; G. BALBI, *I reati contro la libertà e l'autodeterminazione sessuale in una prospettiva di riforma*, in Sist. Pen., 3 marzo 2020; M. BALL, *Metaverso*. *Cosa significa, chi lo controllerà e perché sta rivoluzionando le nostre vite*, G. MANCUSO (Traduzione a cura di), Milano, Garzanti, 2022; F. BASILE, *Intelligenza artificiale e diritto penale: qualche aggiornamento e qualche nuova riflessione*, in G. BALBI, F. DE SIMONE, A. ESPOSITO, S. MANACORDA (a cura di), *Diritto penale e intelligenza artificiale. Nuovi scenari*, Torino, Giappichelli, 2022; F. BOTTALICO, *Il furto di identità digitale*, in G. SICIGNANO, A. DI MAIO (a cura di), *Nuove problematiche in tema di reati informatici*, Milano, La Tribuna, 2022; C. BURCHARD, *L'intelligenza artificiale come fine del diritto penale? Sulla trasformazione algoritmica della società*, in Riv. It. Dir. Proc. Pen., 2019, 62, 4; F. CAMPLANI, *Locus commissi delicti, norme di collegamento e reati informatici a soggetto passivo indeterminato*, in Arch. Pen., 2020, 2; A. CAPPELLINI, *Machina delinquere non potest. Brevi appunti su intelligenza artificiale e responsabilità penale*, in Criminalia, 2018; M. CATERINI, *Il giudice penale robot*, in La legisl. Pen., 19.12.2020; S. CHESTERMAN, *Artificial Intelligence and the problem of Autonomy*, 2019, in Journal on Emerging Technologies, 2020, 1, 2; A. CONTINIELLO, *Le nuove frontiere del diritto penale nel Metaverso. Elucubrazioni metagiuridiche o problematica reale?*, in Giur. Pen. Web, 2022, 5; M. CROCE, *Cyberlaundering e valute virtuali. La lotta al riciclaggio nell'era della distribuited economoy*, in Sist. pen., n. 4, 2021; C. CUPELLO, *La sfida dell'intelligenza artificiale al diritto penale*, in *https://www.sistemapenale.it/it/scheda/cupelli-la-sfida-dellintelligenza-artificiale-al-diritto-penale*, 21 aprile 2023; L. DELLA RAGIONE, *Il delitto di frode informatica: l'art. 640 ter c.p.*, in G. SICIGNANO, A. DI MAIO (a cura di), *Nuove problematiche in tema di reati informatici*, Milano, La Tribuna, 2022; F. DE SIMONE, *L'implementazione delle nuove tecnologie nelle politiche anticorruzione*, in G. BALBI, F. DE SIMONE, A. ESPOSITO, S. MANACORDA (a cura di), *Diritto penale e intelligenza artificiale. Nuovi scenari*, Torino, Giappichelli, 2022; F. DE SIMONE, *I delitti contro l'integrità dei dati dei programmi e dei sistemi informatici: gli attacchi "Denial of Service*, in G. SICIGNANO, A. DI MAIO (a cura di), *Nuove problematiche in tema di reati informatici*, Milano, La Tribuna, 2022; O. DI GIOVINE, *Il "judge-bot" e le sequenze giuridiche in materia penale (intelligenza artificiale e stabilizzazione giurisprudenziale)*, in

[188] O. KOSTENKO, *Electronic jurisdiction, metaverse, artificial intelligence, digital personality, digital avatar, neural networks: theory, practice, perspective*, in World Science Journal, 2022, 73, 2, pp. 10 ss. The author has developed six postulates regarding the Metaverse that could well rise to the status of guiding criteria in the development of shared regulation. In summary he states that: the Metaverse is the technology of cosmopolitan development of humanity; The key subject in the Metaverse is human, but electronic personalities and electronic avatars will be the key to the Metaverse; New technologies need human forms of control and deterrence; the development of biorobots, Android robots, and biomechanical systems and organisms requires the development of ethical norms and legal indicators for the use of these devices; autonomous weapons should not be allowed to attack objects and subjects independently and autonomously; it is necessary to develop norms of E-jurisdiction and E-justice, as key elements of electronic public relations in the Metaverse.

Cass. Pen., 2020; E. DINCELLI, A. YAYLA, *Immersive virtual reality in the age of the Metaverse: A hybrid-narrative review based on the technology affordance perspective*, in The Journal of Strategic Information System, 2022, 31, 2; A. ESPOSITO, *Il cyberbullismo*, in G. SICIGNANO, A. DI MAIO (a cura di), *Nuove problematiche in tema di reati informatici*, Milano, La Tribuna, 2022; G. FIANDACA, G. LEINERI, *Sub art. 6 c.p.*, in FORTI G., SEMINARA S., ZUCCALÀ G., *Commentario breve al codice penale*, Milano, Cedam, 2017; L. FLORIDI, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano, Raffaello Cortina ed., 2017; M. FOUCAULT, *Spazi altri. I luoghi delle eterotopie*, Vaccaro S. (a cura di), Milano, Mimesis, 2001; G. GENTILE, *Il furto di dati informatici*, in G. SICIGNANO, A. DI MAIO (a cura di), *Nuove problematiche in tema di reati informatici*, Milano, La Tribuna, 2022; M. GIALUZ, *Quando la giustizia penale incontra l'intelligenza artificiale: luci e ombre dei risk assessment tools tra Stati Uniti ed Europa*, ivi, 29 maggio 2019; R. GIORDANO, A. PANZAROLA, A. POLICE, S. PREZIOSI, M. PROTO (a cura di), *Il diritto nell'era digitale. Persona, Mercato, Amministrazione, Giustizia*, Milano, Giuffrè, 2022; M. GIUCA, *Criptovalute e diritto penale nella prevenzione e repressione del riciclaggio*, in Dir. pen. cont. riv. trim., 2021; D. INGARRICA, *Metaverso criminale. Quali interazioni nel presente nazionale e quali sfide globali del prossimo futuro*, in Giur. Pen. Web, 2022, 9; O. KOSTENKO, *Electronic jurisdiction, metaverse, artificial intelligence, digital personality, digital avatar, neural networks: theory, practice, perspective*, in World Science Journal, 2022, 73, 2; V. MANES, *L'oracolo algoritmico e la giustizia penale: al bivio tra tecnologia e tecnocrazia*, in U. RUFOLO (a cura di), *Intelligenza artificiale. Il diritto, i diritti, l'etica*, Milano, Giuffrè, 2020; W. MARASCHINI, C. SCAGLIARINI, *Algoritmi in Pascal*, Torino, Paravia ed., 1995; M. MASTROGIOVANNI, *Intermedialità e rimediazione nel metaverso una ricognizione bibliografica ragionata (con qualche proposta)*, in Riv. Interd, Com., 2022, 4; T. OLEKSY, A. WNUK, M. PISKORSKA, *Migration to the metaverse and its predictors: attachment to virtual places and metaverse-related threat, in Computers* in Human Behavior, 2022; C. PARODI, V. SELLAROLI (a cura di), *Diritto penale dell'informatica. Reati della rete e sulla rete*, Milano, Giuffrè, 2020; S.R. PALUMBIERI, *I delitti contro la libertà sessuale* (voce), in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), *Diritto Penale*, Milano, Utet, 2022; G. PICA, *I reati nella società dell'informazione*, in S. ALEO, G. PICA, *Diritto penale. Parte Speciale II*, Padova, Cedam, 2012; L. PICOTTI, *Diritto penale e tecnologie informatiche: una visione di insieme*, in A. CADOPPI, S. CANESTRARI, A. MANNA, M. PAPA (a cura di), *Cybercrime*, Milano, Utet, 2019; C. PIERGALLINI, *Intelligenza artificiale: da 'mezzo' ad 'autore' del reato?*, in Riv. It., Dir. Proc. Pen., 2020; T. PIETRELLA, *Reati informatici e concorso di norme: come l'evoluzione tecnologica informa il diritto penale. Il caso delle botnets*, in Discrimen 2 dicembre 2021; S. RIONDATO, *Robot: talune implicazioni di diritto penale*, in P. MORO, C. SARRA (a cura di), *Tecnodiritto,* Milano, Franco Angeli, 2020; E. RIVA, *Le fattispecie di danneggiamento informatico: una comparazione tra Italia e Cina*, in Sistema pen., 2021, 4; S. RODOTÀ, *Tecnologie e diritti*, Bologna, Il Mulino, 2021; G. SCORZA, *In principio era Internet e lo immaginavamo diverso*, in Riv. It. Inform. Dir., 2022, 1; F. SARZANA DI SANT'IPPOLITO, M.G. PIERRO, I.O. EPICOCO, *Il Diritto del Metaverso. NFT, DeFi, GameFi e privacy*, Torino, Giappichelli, 2022.