Original Research Paper

UDK: 342.738:004.738.5]:341.24

THE METAVERSE AND PRIVACY: NEW CRITICAL ISSUES ON THE HORIZON

Antonio Vertuccio
PhD student
University of Campania 'Luigi Vanvitelli', Caserta, Italy
antoniovert97@gmail.com

1. Introduction

The term "metaverse" has become commonly used as a synonym for an immersive, interconnected and interoperable space capable of changing the ordinary distinction between real and virtual. The metaverse is a large and ambitious project, which for the moment does not exist, and which is characterized by innovative features compared to the virtual worlds we know. It can be understood as an interoperable and large-scale network of three-dimensional virtual worlds represented in real time, which can be experienced in a synchronous and unlimited way by a boundless number of users and with continuity of data.[326] Interoperability assumes a fundamental importance in the construction of this evolution of the "internet", and is embodied in the close interconnection between multiple computer systems. Persistence, meanwhile, is the property that allows the metaverse to operate in such a way that it does not need to be paused. This feature will allow operators to create an immersive and constant space where users can carry out any type of activity.[327] These preliminary definitions allow us to understand how the metaverse will be the sum of all publicly accessible virtual worlds. The achievement of this new form of reality, which will happen in the near to medium term, introduces new critical issues with regard to the protection of the fundamental rights of users. The right to privacy is certainly among those that are most exposed to the dangers associated with the development of this permanent and immersive infrastructure. Indeed, users will be forced to give up a significant amount of personal data in order to access the metaverse. The potential transposition of many individual activities into this virtual network could affect the essence of the right to privacy and its corollaries.

This contribution aims to verify in particular whether current international laws are able to meet the new challenges that the metaverse poses in relation to the protection of the right to privacy. To this end, we will make preliminary references to the way in which the right to privacy is protected in the European Convention on Human Rights (ECHR) and in the Charter of Fundamental Rights of the European Union (section 2). We will then provide a recap of the international sources applicable to the metaverse, and examine whether these rules are able to govern the systemic risks that are on the horizon (from section 3 to

[326] A. MAZZETTI, *Il Metaverso*: *sfide, opportunità e benefici per un mondo digitale immersivo*, in *Metaverso. Diritto degli utenti – Piattaforme digitali – privacy – diritto d'autore – profili penali e NFT*, a cura di G. CASSANO - G. SCORZA, Pacini, 2023, 16 ss.
[327] European Parliamentary Research Service (EPRS), *Metaverse Opportunities, risks and policy implications*, 2022.

section 7). At the same time, we will try to develop a comparison between European and American legislation in order to assess the adaptability of these regulatory systems to the metaverse (section 7).

2. The protection of the right to privacy in the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union

Before proceeding to the analysis of the regulations applicable to the metaverse we will briefly frame the sources that protect the right to privacy, making reference to Article 8 of the European Convention on Human Rights (ECHR)[328] and Articles 7 and 8 of the Charter of Fundamental Rights of the European Union.[329] Article 8 of the ECHR enshrines every person's right to respect for his or her private and family life, home and correspondence. This article stipulates that there be no interference by public authorities with the exercise of that right, unless such interference is provided for by the law and constitutes a measure which is necessary in a democratic society for the pursuit of specific ends.[330] States cannot perpetrate unlawful interference with the privacy of affiliates and have a positive obligation to ensure that the right to privacy is also respected between private individuals.[331] Article 7 of the Charter of Fundamental Rights of the European Union also protects respect for private and family life, while Article 8 of the Charter further outlines the right of every person to the protection of personal data concerning him or her.[332] These data must be processed fairly, for specified purposes and on the basis of the consent of the person concerned, or on some other basis provided for by the law. In addition, every person has the right to access the data that have been collected about him/her, and compliance with these rules is subject to the control of an independent authority.

This framework sets up the regulations that will be examined below, and allows us to better understand them, as well as the points of difficulty with regard to applying them to the metaverse.

3. The European General Data Protection Regulation: a regulatory reference applicable to the metaverse?

The European General Data Protection Regulation (GDPR)[333] has as its legal basis the aforementioned Article 8 of the Charter of Fundamental Rights of the European Union and aims to regulate the processing[334] of personal data of internet users. The GDPR first of all states that personal data must be processed lawfully, transparently, and for specified, explicit and legitimate purposes. In addition, it outlines the principle of data minimization, whose corollary is the need for the data to be adequate, relevant and limited in relation

[328] European Convention on Human Rights, Rome, 4 September 1953.
[329] Charter of Fundamental Rights of the European Union, Nice, 7 december 2000.
[330] "These include safeguarding national security, public order, the economic well-being of the country, the prevention of crime, the protection of health or morals, the protection of the rights and freedoms of others."
[331] European Court of Human Rights, Barbulescu v. Romania, Strasbourg, 5 September 2017.
[332] The legal basis of this Article is provided by Article 286 of the Treaty establishing the European Community, Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data, Article 8 of the ECHR and the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 28 January 1981, ratified by all Member States. Article 286 of the EC Treaty is now replaced by Article 16 of the Treaty on the Functioning of the European Union and Article 39 of the Treaty on European Union. For further information on Article 8 of the Charter of Nice, see: C. Giust., La Quadrature du net and Others v Premier ministre and others, 16 October 2020.
[333] Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of data, Brussels, 27 April 2016.
[334] Pursuant to art. 4 of the GDPR for processing means: "any operation or set of operations, performed with or without the aid of automated processes and applied to personal data or sets of personal data, such as collection, registration, organization, structuring, storage, adaptation, cancellation".

to the purposes for which they are processed. The European Regulation defines biometric data as: "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data". The processing of this data is prohibited pursuant to Article 9 of the GDPR, unless the data subject has given his or her explicit consent or specific circumstances occur.[335] These definitions are of fundamental importance for investigation of the risks to the protection of privacy in the metaverse, as the most commonly acquired data in this new virtual space will be none other than biometric data. We believe that the general principles that have been discussed are applicable to the processing of personal data by the "owners" of the three-dimensional worlds that will make up the metaverse,[336] and constitute the relevant legal basis. At the same time, however, we believe that the question of the GDPR's applicability must take into account the peculiarities that characterize the metaverse. This interoperable space will be characterized by extensive use of artificial intelligence and the acquisition of greater amounts of data than we have previously experienced. Users' consent regarding the acquisition of their sensitive data may even be coerced, since the processing of such data will most likely be the basic condition for access to and use of the possibilities granted by the metaverse.

These circumstances make the provisions of Article 15 of the GDPR even more relevant; these state that the interested party has the right to obtain information about the purposes of the data processing, the categories of personal data, relative recipients, and data retention period. The retention of personal data may also change in the metaverse, given that the persistence and immersiveness of these new virtual spaces could lead to permanent retention of personal data. A further aspect of interest could be the need to regulate profiling mechanisms that may develop in illegitimate ways, due to the use of advanced and innovative technologies. Profiling can be defined as any form of automated processing of personal data aimed at analyzing and predicting users' personal tastes and characteristics. The data subject has the right not to be the recipient of a decision based on automated processing, unless the decision is based on the data subject's explicit consent or authorized by Union or Member State law or is necessary for the fulfillment of a contract.[337] The automated processing of personal data will be central to the metaverse, and this aspect may cause critical issues in regard to how transparently and effectively platforms provide users the possibility to give or withhold their consent. At the same time, the GDPR regulates issues related to the transfer of personal data; however, we believe that the dynamic and fluid mechanics underlying the metaverse will radically change the concept of territoriality, requiring new ways of thinking that take into account the relevant risks.[338]

The applicability of the GDPR to the metaverse is difficult to determine in many respects, given that the metaverse does not currently exist; however, we believe that Article 35 of the GDPR is able to overcome apparent difficulties. Compliance with this norm is a prerequisite condition for the legitimate evolution of the metaverse. The article states that where a new type of processing may result in a high level of risk to the rights and freedoms of natural persons, the controller is required to carry out an impact assessment of the intended processing operations on the protection of personal data. This assessment shall contain at the

[335] Article 9 paragraph 2 of the GDPR stipulates that "the processing of sensitive data is possible if: the data subject has given his or her explicit consent, if the processing is necessary for the purposes of fulfilling the obligations and exercising specific rights of the controller or the data subject in the field of employment law, if the processing is necessary to protect the vital interests of the data subject, if it concerns data made public by the interested party, if the processing is necessary for the establishment, exercise or defence of legal claims, if this is necessary for reasons of public interest."

[336] F. BAVETTA, *Metaverso e protezione dei dati personali*, in *Metaverso. Diritto degli utenti – Piattaforme digitali – privacy – diritto d'autore – profili penali e NFT*, a cura di G. CASSANO - G. SCORZA, Pacini, 2023, wo.cit.., 178 ss.

[337] Article 22 of GDPR

[338] On the problems related to territoriality, see: Hearing at the Senate of the Republic by A. Celotto, The "metaverse" and its implications for the legal system, 2022.

very least a systematic description of the intended processing operations and purposes of the processing, an assessment of the necessity and proportionality of the processing operations in relation to purpose, and an analysis of the risks to the rights and freedoms of the data subjects. In addition, measures to address risks and security measures to ensure the protection of personal data should be outlined as part of the impact assessment. In the event that a high risk is detected, the data controller should consult an ad hoc supervisory authority, which, if there is a failure to mitigate the risk, will provide written advice. Given this provision, it is reasonable to assume that the managers of the various infrastructures that will constitute the metaverse will, either independently or in cooperation, have to develop an impact assessment of the metaverse as regards the protection of personal data. This technical assessment will be fundamentally important, as it will allow us to understand whether the GDPR can provide a suitable legal basis for governing the risks related to the metaverse. We believe that impact assessments should be developed in a way that is compatible with the principle of privacy by design, as enshrined in Article 25 of the GDPR. The principle in question is aimed at including privacy among a platform's default settings and embedding it through the ex ante use of pseudonymization and data minimization techniques. The European Data Protection Board (EDPB)[339] has formulated guidelines on the interpretation of the principle of privacy by design, and clarified its corollaries and the perimeters within which it can maneuver. This independent European body has highlighted that the data controller should choose options and settings for data processing which ensure that only the processing strictly necessary to achieve the specific and lawful purpose is carried out.[340] In addition, the owner is required to define in advance the specific, explicit and legitimate purposes that personal data are collected and processed for. Measures must be adequate to ensure that only data necessary for each specific purpose are processed.[341] In this respect, the EDPB has listed transparency, correctness, lawfulness, accuracy, minimization and integrity as the principles that data controllers must follow in order to tend towards an implementation of privacy by design. This principle seems to have influenced the European Commission, which has presented a statement announcing its intention to present a proposal for the regulation of the metaverse.[342]

The principle of privacy by design and impact assessments could be the normative reference to take into consideration in order to prevent the metaverse from taking an anti-democratic turn that is strongly detrimental to the right to privacy. Failure to enforce these rules could result in the nullification of individuals' privacy prerogative.[343] The principle of privacy by design seems also to underlie other European sources, as we will show.

4. The Proposal for a Regulation on Artificial Intelligence: a valid legislative evolution?

Artificial Intelligence (AI) is one of the pivots on which the metaverse is developing. A macro-distinction could be made between context AI,[344] aimed at guaranteeing the space-time continuum in the metaverse, and functional relational AI and supporting decision-making processes.

[339] The European Data Protection Board (EDPB) is an independent European body that ensures consistent application of data protection rules across the European Union and promotes cooperation between EU data protection authorities.
[340] EDPB, "Guidance 4/2019 on Article 25 Data protection by design and by default", 16 January 2020, available at: edpb.europa.eu.
[341] EDPB, "Guidelines on the necessity and proportionality of measures restricting the right to data protection", 25 February 2019, available at: edps.europa.eu.
[342] European Commission, Statement, Brussels, 14 September 2022. "The three pillars of this new discipline have been identified by the Commission as: people, technologies and infrastructures".
[343] I. BARTOLETTI - I. LUCCHINI, *Privacy nel metaverso, tutelarla o saranno guai*: *ecco perché*, in *agendadigitale.eu*, 2022;
[344] L. BOLOGNINI, *Il futuro dei dati personali nel metaverso*, in *Diritto, Economia e Tecnologie della Privacy*, 2022.

One source that may regulate the use of AI in the metaverse is the Proposed Regulation on Artificial Intelligence.[345] The Proposal establishes harmonized rules for how AI is placed on the market and used within the EU. As part of the Proposal for a Regulation there is a classification of high-risk AI systems,[346] in relation to which a series of requirements to be respected are established. The list of high-risk AI systems may be updated by the European Commission where the systems are used for public purposes and present a risk of negative impact on fundamental rights. In making that assessment, the Commission takes into account the intended purpose of the AI system, and the extent to which persons likely to suffer harm are in a vulnerable position vis-à-vis the user of an AI system, in particular due to an imbalance of power, knowledge, and/or economic or social situation. The Proposal for a Regulation states that a risk management system must be implemented, documented and maintained for high-risk AI systems. This system shall include the identification and analysis of known and foreseeable risks associated with the system and the simultaneous assessment of any other risks arising from the analysis of the data collected by the post-market monitoring system. In addition, suppliers must take appropriate risk management measures to manage this impact assessment. This risk assessment must be reflected in the appropriate design and manufacture of the systems, in the implementation of control measures and in the provision of adequate information to users. At the same time, AI system providers must ensure that logs are recorded during operation.

The reported provisions seem to be closely connected with the principle of privacy by design sanctioned by the GDPR, as they tend towards a systemic prevention of risks related to elastic and nuancedtechnological evolutions. In this perspective, AI system providers should ensure that AI systems are subjectto the relevant assessment procedure before they are placed on the market or put into service. This provisionalso seems to follow similar lines to those established by by the GDPR and tends towards a rationalizationof critical issues in a preventive way aimed at safeguarding fundamental rights. The peculiar characteristicsof the metaverse lead us to believe that this "interoperable world" may be described as a high-risk AI system. From this point of view, the risk management system could mitigate the critical issues related to the creation of this new virtual space, and protect against potential violations of users' right to privacy.

5. The applicability of the Digital Services Act to the metaverse

The Digital Services Act (DSA)[347] establishes harmonized rules on the provision of intermediary services in the internal market and constitutes an important point of reference for the delineation of a technical regulation compatible with dramatic technological evolutions. It accordingly divides intermediation services into mere conduit transport, storage services, and a hosting service.[348] We may have reason to believe that in the middle of the world, the providers of the intermediary will be the creators of the three-dimensional worlds connected in the metaverse, in which case the obligations imposed by the DSA will fall on them.[349] Indeed, the private actors who own these three-dimensional worlds will put in place intermediary services compatible with those stipulated by the DSA. From this perspective, it is likely

[345] European Parliament and Council, Proposal for a Regulation establishing harmonised rules on Artificial Intelligence and amending certain legislative acts of the Union, Brussels, 2021.

[346] Articles 6 and 7 of the Proposal for a Regulation on Artificial Intelligence.

[347] Regulation of the European Parliament and of the Council on a single market for digital services (Digital Services Act) and amending Directive 200/31/EC, Brussels, which entered into force on 16 November 2022.

[348] Article 2 of the DSA clarifies that "simple transport services consist in transmitting over a communications network information provided by a recipient of the service, the caching service consists in transmitting over a communication network information provided by the recipient of the service and involves the automatic and temporary storage of that information and the hosting service consists in the storage of information provided by the recipient at the request of the latter".

[349] G. VACIAGO, *Metaverso e responsabilità delle piattaforme*, in *Metaverso. Diritto degli utenti – Piattaforme digitali – privacy – diritto d'autore – profili penali e NFT*, a cura di G. CASSANO - G. SCORZA, Pacini, 2023, wo. cit., 321 ss.

that these service providers will transmit information provided by the recipient of the service over communications networks and develop storage systems for acquired data.

The legislative source in question establishes additional obligations for very large online platforms (which will include the three-dimensional worlds that make up the metaverse), and requires them to identify and analyze any systemic risks deriving from the design of their service.[350] The DSA outlines an exemplary list of possible systemic risks, referring in particular to the possible dissemination of illegal content, and to any negative effect on the exercise of fundamental rights enshrined in the Charter of Fundamental Rights of the European Union. With this in mind, very large online platform providers are required to put in place mitigation measures that are reasonable, proportionate, effective and appropriate to systemic risks.[351] Among the mitigation measures are those that could be highly effective in the regulation of issues associated with the metaverse. Systems of cooperation between the various suppliers and awareness-raising measures are also defined with the aim of protecting the rights of minors.[352] A crisis response mechanism is also envisaged, the assessment of which is the responsibility of the Commission, which may adopt decisions containing measures for specific, effective and proportionate repairs.[353] Large online platforms are subject to checks by independent organizations to verify whether commitments that exist under the combined legislation are being met. In addition, platforms are required to appoint one or more compliance officer to monitor the platforms' compliance with the Regulation.

The articles in question are characterized by a higher level of technicality, and are more suitable for standardizing the dynamic issues that characterize the digital world.[354] This assumption is evidenced by the fact that the Regulation places obligations directly on intermediation services. The constant reminder of the need to make assessments about the risks that lie ahead is entirely compatible with the new and unknown implications of the metaverse. At the same time, the reference to the need to assess possible risks regarding the protection of fundamental rights and public security outlines a regulatory framework within which the different expressions of the metaverse must remain, in a perspective compatible with the need for sustainable development.[355] We believe that these rules are fully applicable to the metaverse, and subordinate its development to the protection of users' fundamental rights.

6. Inferred data: critical issues and perspectives

In a declaration[356] issued in 2019, the Council of Europe highlighted how machine learning and artificial intelligence are regularly using inferred data. Inferred data are data taken from other data which, if used on a large scale, can influence not only the behavior but also the choices, opinions and emotions of citizens. These are essentially massive forms of profiling of individual and collective behavior. The processing of these data could lead to the definition of surveillance and profiling models based on the analysis of expressions on the faces and gestures of our avatars. Information that derives and conceptually depends on

[350] Article 25 and 26 of Digital Service Act.
[351] Article 27 of Digital Service Act.
[352] Article 27 of Digital Service Act.
[353] Article 37 of Digital Service Act.
[354] P. BONINI, *Il* "*metaverso*". *Questioni e prospettive di diritto costituzionale*, 2022.
[355] On sustainability, see: C. FOCARELLI, *La sostenibilità nel diritto internazionale*: *spunti dalla* prassi *più recente*, in *Rivista di diritti comparati*, 2022, 350 ss.
[356] Council of Europe Declaration "on the manipulative capabilities of algorithmic process", Strasbourg, 2019.

psycho-physical data is used to elaborate such models.[357] These circumstances increase the risk of influencing the behavior and political choices of users.

Inferred data will become increasingly important in the metaverse, and, following the sources we have referred to, it is necessary to use countermeasures to combat the anti-democratic drift to which the processing of these data could lead. The Council of Europe has highlighted the need to promote a broad discussion regarding the challenges that digital evolution poses for the law; secondly,[358] it has recommended the adoption of measures to ensure adequate, appropriate and proportionate safeguards. Finally, the Council has recommended that Member States promote critical scientific studies with a view to deepening knowledge and raising awareness of the ways in which personal data are generated and processed.

The findings of such studies highlight how one of the dangers associated with technological evolution is the creation of a mass surveillance system capable of directly and indirectly governing the choices of users. The Council of Europe's references to social conscience regarding data processing procedures seem not to be purely legal, but actually, in the opinion of this writer, represent the material substrate necessary to make European and International standardization fully effective.[359] This will need to be further strengthened.

7. The Digital Platform Commission Act and the metaverse: comparisons with European law

As regards American legislation, the US Congress[360] enacted the "Digital Platform Commission Act of 2022",[361] with which it tried to moderate content on digital platforms. With this legislative act it was noted that all digital platforms are unregulated and have developed unfair practices that have resulted in demonstrable violations of the rights of users.[362] Through this act, Congress created a Federal Commission for Digital Platforms whose primary task is to protect consumers from deceptive, unreasonable and unauthorized practices committed by digital platforms. The Commission assesses the fairness of the algorithmic processes of online platforms and puts in place supervisory powers over the management of the activity of the platforms themselves. In addition, the Commission is empowered to designate systemically important digital platforms in specific circumstances.[363]

The enactment of the Digital Platform Commission Act may be a prelude to developing more insightful control of the practices developed by digital platform operators. The powers given to the Commission seem to point in this direction and may allow effective supervision of algorithmic processes. Indeed, this legislation tends to limit the self-determination of private actors (stakeholders) who own digital platforms and will monopolize the metaverse.

Comparison of American legislation with European legislation may lead to the import of the "systemic model" of privacy protection in force in Europe into the American legal system. As stated above, the

[357] F. BAVETTA, *Metaverso e protezione dei dati personali*, in *Metaverso. Diritto degli utenti – Piattaforme digitali – privacy – diritto d'autore – profili penali e NFT*, a cura di G. CASSANO - G. SCORZA, Pacini, 2023, wo.cit., 185 ss.

[358] On digitalization, see: G. De Gregorio-R. Radu, *Digital constitutionalism in the new era of Internet Governance*, in *International Journal of Law & Information Technology*, 2022, 68 ss.

[359] On the social distortions relating to the transfer of personal data, see: B. CARAVITA, *Principi Costituzionali e Intelligenza artificiale*, in *Intelligenza artificiale. Il diritto, i diritti, l'etica*, a cura di U. Ruffolo, Giuffrè, 2020, 451 ss.

[360] The United States Congress is the legislative body of the United States federal government.

[361] The Digital Platform Commission Act is a bill enacted by Congress on 05/12/2022, available at: www.congress.gov.

[362] Among the demonstrable damages in point 6 of the Digital Platform Commission Act we find "violations of privacy and virtual dependence created against minors".

[363] The circumstances are as follows: "Opening the platform to the public, significant involvement of users, carrying out inter-state activities and the development of operations with economic impact".

European regulatory framework seems to be coherent and adequate for managing the transitional phase that currently characterizes development of the metaverse. The promulgation of the Digital Service Act does not mean that a standard of protection similar to that available in Europe has been defined; however it certainly constitutes a significant step forward for the regulation of the activity of platform operators. A further important development in American legislation may take the form of effective acceptance of the principle of privacy by design.

Conclusions

This study has analyzed the systemic risks that the metaverse poses to the protection of the right to privacy. To this end we reconstructed the definition of metaverse and explored the international sources that protect the right to privacy. Subsequently, we summarized the European regulations applicable to the metaverse, evaluating their intrinsic effectiveness. Reference was made here to the serious danger represented by inferred data. Finally, we analyzed the American sources applicable to the metaverse, examining these in comparison with European regulations.

The advent of the metaverse will radically change our current conception of the right to privacy and its corollaries, as individuals transpose huge amounts of data into online three-dimensional worlds. This will have a decisive influence on the protection of the right to privacy and will lead to new and complex scenarios. In this perspective, imminent digital privatization requires a strong legal effort aimed at preventing technological evolution from dissolving the law. These contemporary challenges require hermeneutical efforts characterized by the intrinsic awareness that the law is the only tool for preventing drifts that are not only detrimental to the right to privacy, but also to human dignity.

We believe that the sources analyzed above can allow us to manage the on-going transitional phase while protecting the right to privacy. In this sense, we hope that the principle of privacy by design and the related impact and risk assessments will effectively be the regulatory core for safeguarding users from the risks associated with the metaverse. Failure to comply with these regulations could result in violations of the right to privacy that would be difficult to remedy in the future. The regulation of today's transitional phase could be a prelude to effective management of systemic risks related to the metaverse.

Reference List

1. A. MAZZETTI, *Il Metaverso*: *sfide*, *opportunità e benefici per un mondo digitale immersivo*, in *Metaverso. Diritto degli utenti – Piattaforme digitali – privacy – diritto d'autore – profilipenali e NFT*, a cura di G. CASSANO - G. SCORZA, Pacini, 2023.
2. BARTOLETTI - I. LUCCHINI, *Privacy nel metaverso, tutelarla o saranno guai*: *ecco perchè*, in *agendadigitale.eu*, 2022.
3. F. BAVETTA, *Metaverso e protezione dei dati personali*, in *Metaverso. Diritto degli utenti – Piattaforme digitali – privacy – diritto d'autore – profili penali e NFT*, a cura di G. CASSANO - G. SCORZA, Pacini, 2023.
4. L. BOLOGNINI, *Il futuro dei dati personali nel metaverso*, in *Diritto, Economia e Tecnologie della Privacy*, 2022.
5. P. BONINI, *Il "metaverso". Questioni e prospettive di diritto costituzionale*, 2022.
6. B. CARAVITA, *Principi Costituzionali e Intelligenza artificiale*, in *Intelligenza artificiale*. *Il diritto, i diritti, l'etica*, a cura di U. Ruffolo, Giuffrè, 2020.
7. C. FOCARELLI, *La sostenibilità nel diritto internazionale*: *spunti dalla* prassi *più recente*, in *Rivista di diritti comparati*, 2022.

8. G. DE GREGORIO-R. RADU, *Digital constitutionalism in the new era of Internet Governance*, in *International Journal of Law & Information Technology*, 2022.
9. MAZZETTI, *Il Metaverso*: *sfide*, *opportunità e benefici per un mondo digitale immersivo*, in *Metaverso. Diritto degli utenti – Piattaforme digitali – privacy – diritto d'autore – profili penali e NFT*, a cura di G. CASSANO - G. SCORZA, Pacini, 2023
10. G. VACIAGO, *Metaverso e responsabilità delle piattaforme*, in *Metaverso. Diritto degli utenti – Piattaforme digitali – privacy – diritto d'autore – profili penali e NFT*, a cura di G. CASSANO - G. SCORZA, Pacini, 2023.