INFLUENCER MARKETING IN THE METAVERSE ERA, BETWEEN INNOVATION AND DATA PROTECTION

Beatrice Rabai*

SUMMARY: 1.- Introduction; 2.- EU law and new technologies: the development of governance and regulatory strategies; 3.- Influencer marketing and data protection; 4.- (*following*) Metaverse and virtual influencers, between challenges and critical issues; 5.- Conclusion.

1.- **Introduction.**

Information and communication technologies (ICTs) have advanced so quickly during the last three decades that they have changed many facets of society. Producers and service providers have employed these technologies to improve the efficiency and quality of their business operations. People have benefited greatly from this, which has improved their quality of life and given them more chances in many numerous other areas.

One of the main links between the physical and digital applications made possible by the so-called Fourth Industrial Revolution[1] is the Internet of Things (IoT), which is defined as any device connected to the internet for communication and data analysis using sensors, software and numerous other means of connecting things[2].

Remote control, convenience, more individualised service, and unique and creative consumer goods and services are just a few of the many potential advantages that the more recent ICTs – which concentrate on artificial intelligence (AI), cloud computing, machine learning, nanotechnology, blockchain, big data analytics, and other fields – offer to collectivity. Thus, the way we manage our lives has been significantly changed by new technologies. New data-driven technologies have led to substantial advancements in artificial intelligence (AI), particularly in the field of automating formerly human-performed operations.

The COVID-19 epidemic has increased the usage of artificial intelligence and data sharing, which has increased and generated new risks, as we will see later. The literature indicates that ICT is becoming a necessary component of all activities, even the most ordinary ones, to the point that it is now required to promote personal growth, universal development, and societal well-being[3].

As technology becomes more integrated into people's lives, it ends to be just technology and becomes a subject of study for academics, particularly those working in the field of public law, who are

* Assistant Professor of Public Law at the University of Sassari, Department of Law.

[1] It was the idea in Klaus Schwab's book *The Fourth Industrial Revolution*, in *World Economic Forum*, Geneva 2016, which asserts that global society is entering a new phase of development, one in which disruptive technologies (artificial intelligence, autonomous vehicles and the internet of things) are merging with humans' physical lives.

[2] According to M. Javaid, A. Haalem, R. Pratapsingh, R. Suman, E. Santibanez Gonzales, *Understanding the adoption of Industry 4.0 technologies in improving environmental sustaibility*, in *Sustainable Operation and Computers* 3 (2022) 203, «Industry 4.0 technologies empower to connect all stakeholders, in addition to raw material and products, into a resource for sustainability and future growth. There is a requirement to study the capabilities of Industry 4.0 technologies in sustainable environmental aspects. Investors, customers, the media, regulators, and other stakeholders are putting growing pressure on companies to consider their environmental impacts and respond to them».

[3] L. Floridi, *La quarta rivoluzione. Come l'infosfera sta trasformando il mondo*, Milano 2017, 1-7.

responsible for examining advances in technology and issues to ensure that they do not compromise the freedoms and rights of citizens.
Building on this assumption, this contribution aims to examine the legal implications of influencer marketing and to emphasize the need for specific regulation of this phenomenon, with particular focus on the challenges posed by virtual influencers within the Metaverse, especially regarding the protection of users' fundamental rights and freedoms.
Following this introduction, the second section will explore how the European legal framework has evolved to safeguard the fundamental rights of users and consumers while fostering innovation and the adoption of emerging technologies.
The third section will analyze influencer marketing and its legal implications, particularly from the standpoint of protecting followers' personal data.
The fourth section will highlight the complex challenges in balancing the development of the Metaverse and virtual influencers with the protection of users' fundamental rights.
Finally, the fifth section will offer general reflections on how the European Union can achieve its goal of creating a competitive digital market while ensuring the protection of individuals' rights, freedoms, and personal data.

2.- **EU law and new technologies: the development of governance and regulatory strategies.**

Recently, innovation has become a key element of the Union's strategy for economic growth.
The European Commission has declared that «innovation is essential to stimulate Europe's competitiveness and guarantee the health and well-being of its citizens. Innovation shapes markets, transforms economies, stimulates radical changes in the quality of public services and is essential to achieve the general objectives of the dual green and digital transition»[4].
Digital technology empowers those who have access to it. Additionally, it greatly enhances communication and creates new avenues for human action. In order to keep up to the United States in terms of technological growth, European politicians have historically placed a high priority on encouraging innovation.
Although technological advancements are crucial for improving the economy, society, and environment, they also provide new risks and vulnerabilities which create significant difficulties for the national legal systems of Europe[5].
Citizens may face issues with these new developments in the areas of accountability and interoperability, privacy and security, transparency and disclosure, and inequity and discrimination[6].
Therefore, governments face an important issue: how to ensure fair markets, uphold rules, and

[4] European Commission, *A New European Innovation Agenda. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions*, COM (2022) 332 final.
[5] As said E. Palmerini, *The interplay between law and technology, or the RobotLaw project in context*, in E. Palmerini, E. Stradella (eds.), *Law and Technology. The challenge of regulating Technological Development*, Pisa 2013, 8, «challeging traditional legal categories and qualifications, posing risks to fundamental rights and freedoms that have to be considered, and more generally demanding a regulatory ground on which they can be developed and eventually launched».
[6] See H. Micklitz, O. Pollicino, A. Reichman, A. Simoncini, G. Sartor, G. De Gregorio (eds.), *Constitutional Challenges in the Algorithmic Society*, Cambridge 2021, 5ss.

safeguard citizens' fundamental rights and freedoms while enabling the growth of these new technology and businesses?

According to this viewpoint, the role of law and regulation is essential for managing the tension between innovation and risk by maintaining a high degree of protection, providing safety nets, and assigning responsibility for any negative effects[7].

Governments and European institutions must direct new and emerging technologies so that they support inclusive and sustainable development and «leave no one behind»[8] since innovation, economic progress, and well-being are closely linked.

The role of legislators, both at the national and European levels, involves continuously reassessing the delicate balance between the unequivocal protection of fundamental rights and freedoms and the promotion of technological development and innovation.

Focusing on personal data and privacy, the rapid expansion of digital and information technologies in recent years has led to systems capable of storing, cross-referencing, and processing – notably through algorithmic means – not only individual data but also data concerning large groups of people. These systems profile individuals based on characteristics such as age, gender, social *status*, ethnic origin, and more. This, in turn, heightens the risk that data collected for legitimate, specific purposes may be misused or exploited in unlawful ways[9].

In a careful balance between the interest of access to personal information (broadly understood) and the security of the information itself, this final point, which unifies the legal requirements of the European Union for the creation of a single digital market, has led to the creation of a number of functional tools to respond to various phenomena and needs, including those relating to the protection of the so-called digital profile.

The General Data Protection Regulation (henceforth referred to as GDPR), EU regulation n. 679 of April 27, 2016, becomes essential in this regard[10]. The idea of data ownership is specifically left in

[7] In these terms M. Weimer, L. Marin, *The Role of Law in Managing the Tension between Risk and Innovation: Introduction to the Special Issue on Regulating New and Emerging Technologies*, in *European Journal of Risk Regulation* 3 (2016) 469-74.

[8] See UN General Assembly, *Transforming our world: the 2030 Agenda for Sustainable Development*, 21 October 2015, A/RES/70/1, avaible at https//www.refworld.org/docid/57b6e3e44.html.

[9] On the topic see L. Friedman, *The Republic of Choice. Law, authority and Culture*, London 1990, 184; J. Rosen, *The Unwanted Gaze. The Destruction of Privacy in America*, New York 2000, 20; P.E. Agree, M. Rotenberg, *Technology and Privacy. The New Landscape*, Cambridge 2001, 7.

[10] On the theme see, in the national context, B. Ponti, *Attività amministrativa e trattamento dei dati personali: gli standard di legalità tra tutela e funzionalità*, Milano 2023; P. Aurucci, *Il trattamento dei dati personali nella ricerca biomedica: problematiche etico-giuridiche*, Napoli 2023; A. Adinolfi, A. Simoncini (ed.), *Protezione dei dati personali e nuove tecnologie: ricerca interdisciplinare sulle tecniche di profilazione e sulle loro conseguenze giuridiche*, Napoli 2022; G. Cassano (ed.), *Il processo di adeguamento al GDPR*, Milano 2022; P. Stanzione (ed.), *I poteri privati delle piattaforme e le nuove frontiere della privacy*, Torino 2022; A. Pajno, F. Donati, A. Perrucci (eds.), *Intelligenza artificiale e diritto: una rivoluzione? Vol.I, Diritti fondamentali, dati personali e regolazione*, Bologna 2022; G. Alpa, *Il diritto di essere se stessi*, Milano 2021, spec. 253ss.; S. Scagliarini, *La tutela della privacy e dell'identità personale nel quadro dell'evoluzione tecnologica*, in *Consulta Online* 2 (2021) 489ss.; M. Bombardelli, *Dati* cit. 352ss.; E. Pellecchia, *Dati personali, anonimizzati, pseudonomizzati, deidentificati: combinazioni possibili di livello molteplici di identificabilità nel GDPR*, in *Nuove leggi civ. comm*., 2020, 360ss.; F. Rossi Dal Pozzo, *Il mercato unico digitale europeo e il regolamento UE sulla privacy*, in R. Cavallo Perin, D.U. Galetta (ed.), *Il diritto dell'amministrazione pubblica digitale*, Torino 2020, 43-45; R. Panetta (ed.), *Circolazione e protezione dei dati personali, tra libertà e regole del mercato. Commentario al Regolamento UE n. 2016/679 (GDPR) e al novellato d.lgs. 196/2003 (Codice Privacy)*, Milano 2019; C. Colapietro, *Il diritto alla protezione dei dati personali in un sistema delle fonti multilivello*, Napoli 2018; A. Pisapia, *La tutela per il trattamento e la protezione dei dati personali*, Torino, 2018; S. Calzolaio, *Protezione dei dati personali*, in *Dig. disc. pubbl., sez. pubbl.*,

favour of settling close attention to the duties to protect the rights of the subjects to whom the data applies, the responsibility profiles of the data controller (*accountability*), the topic of expressed consent and, lastly, to the protection techniques based on a preventive approach (*privacy by design* and *privacy by default*), even though this is in accordance with the previous directive no. 94/46/EC, which outlined the fundamental principles regarding the processing of personal data and their free circulation.

This entails that the potential risks associated with data processing are to be assessed not only in terms of possible infringements of fundamental rights, but also, more broadly, with regard to the protection of the public interest. In other words, risk assessment must take into account both the likelihood of rights violations and the broader implications for the collective interest.

This dimension constitutes one of the most critical aspects of our analysis. It is essential to recall that, in the initial stages, European governments tended to prioritise scientific and technological advancement over the protection of individual rights and freedoms.

Such an orientation was largely driven by the digital economy's structural relevance and the European Union's imperative to remain competitive "vis-à-vis" non-European actors in the global digital market. However, once it became apparent that the digital sphere was inherently difficult to regulate, and that emerging technologies raised substantial legal and ethical concerns, the European Union began to shift its focus.

In recent years, it has sought to establish a more balanced framework aimed at ensuring the effective protection of fundamental rights and freedoms within the evolving landscape of the digital economy and digital society.

At both the national and European levels, this new policy direction has compelled the EU to adopt a distinctive perspective on the relationship between the innovation process and public action. Recent European legislative interventions that move in this direction include the General Data Protection Regulation (GDPR), the Digital Services Act (DSA)[11], the Digital Markets Act (DMA)[12], the Data Governance Act (DGA)[13], the Media Freedom Act (MFA)[14], and the AI regulation (AI Act)[15]. The objective of all of them is to establish a new legal framework for services that protects the fundamental rights of users, promotes fair competition, and prohibits unfair competition that might block innovation, damage small businesses, and limit options for consumers.

agg. VII, Torino 2017, 594-612; G. Busia, L. Liguori, O. Pollicino (ed.), *Le nuove frontiere della privacy nelle tecnologie digitali*, Canterano, 2016.

[11] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC.

[12] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828.

[13] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724.

[14] Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU.

[15] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828. On this theme, see F. Donati, *La protezione dei diritti fondamentali nel regolamento sull'intelligenza artificiale*, in *AIC* 1 (2025) 1ss.

3.- **Influencer marketing and data protection.**

As mentioned above, the development of information and communication technologies has brought about significant progress that has given rise to a new social dimension of individuals, referring specifically to the function that people play when engaging with social networks[16].

In this new digital dimension, it has become more important to publicly share significant aspects of one's life than to quietly enjoy personal space and the right to privacy. Some individuals are more prone to crossing the delicate boundary between public and private spheres by promoting themselves and revealing more personal information on social media than they would likely be willing to share in offline life.

Many engage in this process of spectacularizing their experience within digital platforms by shaping their self-identities to adopt alternative social personas, with the ultimate aim of gaining approval and consensus – typically expressed through likes – from other internet users.

Furthermore, it is clear that this dynamic has played a crucial role in the rise and success of influencer marketing, a novel online business model where companies hire bloggers, social reviewers, or endorsers – generally known as influencers, who aim to gain visibility through the digital platform provided by social networks.

This strategy seeks to boost the visibility of specific sponsored products and, consequently, increase sales. However, influencer marketing is much more than a mere partnership between popular social media users and companies promoting their goods and services.

The power of this marketing approach lies in influencers' ability to rapidly attract large followings on platforms such as Instagram, YouTube, Facebook, Twitter, and more recently, TikTok. Due to their charisma and expertise on certain topics or interests, these influencers' followers are naturally inclined to be influenced by their opinions and recommendations.

This influence, coupled with its potential impact on users' fundamental rights, raises complex legal questions beyond the social and psychological dimensions of this new business model. Only recently have legislators and regulators at both national and European levels begun to address issues related to consumer protection, privacy rights, fair competition, unfair commercial practices, and importantly, data security and personal data protection.

To safeguard consumers from associated risks and harms, these issues must be thoroughly examined and regulated, even though complete resolution may be challenging. The GDPR offers crucial support in this regard, particularly in protecting personal data until comprehensive legislation specifically addressing influencer marketing is enacted.

Therefore, after outlining the privacy and data protection risks, as well as the context in which influencer marketing has evolved, it is essential to clarify which legal principles apply to activities involving influencers.

To better understand the potential challenges posed by influencer marketing, it is important to note that when an influencer publishes content on social media – be it opinions, images, or videos – their

[16] See S. Faro, N. Lettieri, *Big Data e internet delle cose: opportunità, rischi e nuove esigenze di tutela per gli utenti della rete*, in L. Ruggieri, C. Perlingeri (eds.), *Internet e diritto civile*, Napoli 2015, 279-306; M. Flyverbom, R. Deibert, D. Matten, *The Governance of Digital Technology, Big Data and the Internet: New Roles and Responsibilities for Business*, in *Business & Society, Sage* 58.1 (2019) 6; M. Ramajoli (ed.), *Una giustizia amministrativa digitale?*, Torino 2023, and, if you want, B. Rabai, *I big data nell'ecosistema digitale: tra libertà economiche e tutela dei diritti fondamentali*, in *Amministrare* 3 (2017) 407ss.

followers, and even detractors, are free to share or comment on it. However, if the influencer intends to use followers' information for marketing purposes or to transfer it to the company they promote, they automatically assume the role of a data controller and become subject to the GDPR's rules and principles.

For European privacy regulations to apply, the influencer must process followers' personal data, defined by the GDPR as «any information relating to an identified or identifiable natural person ("data subject"); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to more specific elements of his or her physical, physiological, genetic, mental, economic, cultural, or social identity»[17].

Therefore, in the event that personal data are processed, the information will play a fundamental role in the architecture of its protection as a preventive, minimum and essential condition for the lawfulness of the processing (since the interested party learns from the data controller the necessary information to the exercise of one's rights[18]) and the consent of the interested party.

When an influencer begins using the personal data they have collected for business purposes – such as marketing activities like sending commercial communications or profiling, which involves mapping followers' tastes and preferences to target brand companies – they assume the role of data controller.

Therefore, data processing regulations must be applied, even if the influencer initially obtained the follower's information voluntarily. This is because the law focuses on the (new or modified) purpose for which the data is processed[19].

If an influencer intends to reuse sensitive personal data – such as information about political or religious beliefs, health *status*, or similar – beyond standard personal data processing, explicit consent must be obtained from the user, ensuring they fully understand the reasons for this reuse.

To prevent potential data breaches that could negatively affect individuals' rights and freedoms, influencers must carefully assess the risks associated with their data processing activities and the IT systems they employ. This proactive approach helps to mitigate threats such as data theft, unauthorized access, data alteration, denial of access, and unauthorized disclosure, considering the context and manner in which they operate.

4.- (*following*) Metaverse and virtual influencers, between challenges and critical issues.

The need to regulate influencer marketing becomes even more pressing when considering the risks and challenges users face when interacting with virtual influencers operating within the Metaverse – a three-dimensional, fully immersive cyberspace accessible via the Internet, where users navigate

[17] Art. 4 GDPR.

[18] According to art. 4, no. 7, GDPR, «"controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law».

[19] Regarding the treatment of special categories of personal data see art. 9, GDPR.

through avatars (virtual representations of themselves)[20], conduct social and commercial activities, and more[21].

The Metaverse is a digital environment composed entirely of data and information. It is distinct from the physical world, yet it serves as a virtual counterpart where a parallel existence[22] – complete with similar opportunities, limitations, and social dynamics – can unfold[23].

Within this context, influencer marketing has evolved into a unique form of commercial communication.

During the COVID-19 pandemic, many businesses began employing virtual influencers – characters created using computer-generated imagery (CGI) – due to restrictions and the need to reduce costs. These virtual beings, often powered by robots and AI systems, engage audiences and promote products in innovative and cost-effective ways.

One of the primary concerns regarding the Metaverse is the collection and processing of both personal and non-personal data. As in the physical world, such data processing requires explicit user consent to comply with GDPR's transparency and visibility standards. Particularly sensitive personal data – such as biometric or health-related information – can only be processed with clear user consent. Following collection, data must be stored anonymously by default or aggregated in groups. However, ambiguity surrounding the mechanism of obtaining explicit consent, combined with the complexities of processing vast amounts of data through algorithms, fuels ongoing criticism about privacy protection within the Metaverse – a digital environment still not fully understood.

Cybersecurity risks present another critical challenge affecting virtual influencers and their users. Virtual influencers, especially CGI-based ones that can learn autonomously from user interactions without constant human oversight, are vulnerable to cyberattacks. A hypothetical attack that compromises or suspends a virtual influencer's account could have severe repercussions for the influencer, associated companies, and their followers.

Common cyber threats include ransomware – malicious software designed to lock digital devices and extort ransom payments – and phishing, which employs deceptive techniques to trick users into divulging sensitive information such as credit card numbers and passwords. Phishing can result in digital identity theft, unauthorized access to banking information, or the unlawful acquisition of personal data without consent[24].

---

[20] On this theme see F. Bavetta, *Metaverso e protezione dei dati personali*, in G. Cassano, G. Scorza (eds.), *Metaverso. Diritti degli utenti, piattaforme digitali, privacy, diritto d'autore, profili penali, blockchain e NFT*, Pisa 2023, 174ss.

[21] According to A. Liyanaarachchi, M. Mifsud, G. Viglia, *Virtual influencers and data privacy: Introducing the multi-privacy paradox*, in *Journal of Business Research* 176 (2024) «originally, the word is a crossword made up of the terms "meta" (i.e., beyond) and "universum" (i.e., all things, everybody, all people, the whole world), which was later assembled into "metaverse" (meta and universe). The metaverse is, therefore, a meta-universe, a universe that goes beyond the one we know. Journalists, practitioners, and academics now use this word to refer to any structured and open virtual world». See also «*Metaverse Opportunities, risks and policy implications*», a document of the European Parliament Research Service in June 2022, according to which Metaverse is «an immersive and constant virtual 3D world where people interact by means of an avatar to carry out a wide range of activities. Such activities can range from leisure and gaming to professional and commercial interactions, financial transactions or even health intervention such as surgery».

[22] The American business Linden Lab and its creator, Philip Rosedale, recognized its extent and used it to characterize it in 2003.

[23] On the theme, see A. Iannuzzi, *Metaverso, Digital Twins e diritti fondamentali*, in *Rivista it. inf. dir.* 2 (2024) 41 ss.; Cassano, Scorza (eds.), *Metaverso* cit. 5ss.; P. Kotler, *Social media marketing. Marketer dal phygital al metaverso*, Milano 2022; A. Tommasini, *Criptovalute, NFT e metaverso: fiscalità diretta, indiretta e successoria*, Milano 2022.

[24] On the crime of phishing see D. Hummer, J.M. Byrne (eds.), *Handbook on Crime and Technology*, Cheltenham 2023.

The prevalence of these threats and the urgent need for national cybersecurity measures have recently prompted the establishment of a dedicated task force, represented by agencies such as the ACN and the GPDP. This task force aims to promote initiatives focused on national cybersecurity and personal data protection, with the dual objective of safeguarding users' fundamental rights and advancing digital technologies, infrastructure, and skills – key priorities within the European digital strategy[25].
It is noteworthy that European institutions have begun to pay special attention to the Metaverse phenomenon. To guide the upcoming technological transition and ensure an open, secure, reliable, equitable, and inclusive digital environment for EU consumers, businesses, and public administrations, the European Commission launched a new strategy on Web 4.0 and virtual worlds in July 2023. In line with this approach, the European Parliament adopted the Resolution of 17 January 2024 on Virtual Worlds: Opportunities, Risks, and Strategic Implications for the Single Market, which highlights governance challenges arising from the development of virtual worlds.

5.- **Conclusion.**

The development of the economy, society, and the environment is intrinsically linked to technological advancements; however, these advancements also introduce new risks and vulnerabilities that present significant challenges to the national legal systems within Europe. Innovation is a necessary response to an increasingly competitive and globalized world; however, this public good also serves as a tool marked by uncertainty and risk.
Consequently, it necessitates regulatory frameworks that, on the one hand, safeguard technological innovation and, on the other, ensure a level of security that cultivates public trust – an element that is essential for the widespread deployment and adoption of emerging technologies. Innovation, economic growth, and societal well-being are deeply interwoven, thereby compelling European governments and institutions to actively promote nascent technologies that foster inclusive and sustainable development, ensuring that no demographic is marginalized.
Nevertheless, public regulators at both the national and European levels must strike a delicate balance between the protection of fundamental rights and freedoms and the imperative of technological progress. It is only recently that national and European authorities and legislators have begun to address novel online marketing strategies, particularly those centered around influencers – phenomena that warrant close monitoring.
The postponement of legislative and regulatory measures capable of detecting illegal activities and cybercrime is no longer tenable if users are to be assured the security and peace of mind that underpin liberal-democratic societies, even within digital domains.
The reason for this is that the current scope of cybersecurity and privacy only covers a portion of the phenomenon of influencer marketing.
The role of national and European legislators might be described in this way as a constant balancing act between the advancement of technology and the need to safeguard fundamental freedoms and rights. A new legal framework for digital services that respects the aforementioned rights appears to be the goal of the European legislators' recent interventions, which are exemplified by DSA, DMA, DGA, MFA and AI Act.

[25] On the connection between personal data and cybersecurity (and thus national security) see the interesting analysis of P. Stanzione, *Cybersicurezza e protezione dei dati personali*, in *this Journal* 2 (2025) 76ss.

However, some regulatory processes take a long time to implement (given how quickly and unstoppably technology is developing), which may be detrimental to users and, in certain situations, the most vulnerable populations. In this sense, the State, regional governments, regional and local organisations and independent administrative entities can all play a significant role at the national level. There are already a number of initiatives (in terms of soft law) aimed at regulating phenomena related to new technologies (consider the role of the Antitrust Authority or the Agcom guidelines on influencer marketing) and supporting programs that encourage computer literacy and digital education of citizens in order to close the digital divide and help people advance in the digital sphere. People could become more knowledgeable about the benefits and risks of the digital world as a result of this. This would be the first step in protecting their data and experiences from outside influences and cyber threats.
The actions envisaged by the PNRR are particularly significant also because they aim to modernise our country, increase economic prosperity and increase industrial power, while offering citizens the opportunity to fully engage in society, taking advantage of the opportunities offered by new technologies in a context of greater digital awareness, since this is the first weapon that citizens-users can use to prevent risks and dangers in the real world, as well as in the digital one.

Abstract.- Il presente contributo si propone di indagare la complessa interrelazione tra innovazione tecnologica e tutela dei dati personali, con particolare attenzione alle implicazioni giuridiche dell'"influencer marketing" nel contesto del Metaverso. L'analisi intende mettere in evidenza le lacune normative che attualmente caratterizzano questo fenomeno emergente e sottolineare l'urgente necessità di un quadro regolatorio specifico, in grado di affrontarne in modo coerente ed efficace le molteplici sfide.

This paper seeks to investigate the complex interplay between technological innovation and the protection of personal data, with particular emphasis on the legal implications of influencer marketing within the Metaverse. The analysis aims to shed light on the normative gaps currently characterising this emerging phenomenon and to underscore the urgent need for a dedicated regulatory framework capable of addressing its multifaceted challenges in a coherent and effective manner.