The future of personal data in the Metaverse

By **Luca Bolognini**[1] (L.Bolognini@istitutoprivacy.eu) and
Marco Emanuele Carpenelli[2] (M.Carpenelli@istitutoprivacy.eu)

April 5, 2022

Open Access Paper
DOI 10.5281/zenodo.6413046

Incipit

Let's imagine a scenario in a very distant future, several hundred years from now, taking place on another planet, like Mars, where human scholars and intellectuals would be living and studying the history of mankind and its existential, ontological, cultural and social paradigms as they evolved through the centuries on planet Earth. In this scenario, let's also imagine that these scholars were seeking to identify the core of human nature, from ancient Greece to the 21st century based on only 2 historical pieces of information available to them: the Book I of Aristotle's Politics, a work dating back to the 4rth century BC, and the Metaverse video presented by Mark Zuckerberg at the online "Connect2021" event.

[1] President of the Italian Institute for Privacy and Data Valorisation (Istituto Italiano per la Privacy e la Valorizzazione dei Dati – Rome – Italy)
[2] Fellow of the Italian Institute for Privacy and Data Valorisation (Istituto Italiano per la Privacy e la Valorizzazione dei Dati – Rome – Italy)

Would their conclusions based on Aristotle's book be widely different from those based on Zuckerberg's presentation? We believe not.

Aristotle, one of the greatest philosophers of ancient Greece, thought that human beings were innately social animals, irresistibly driven by a primal instinct to communicate, share, socialise, and associate with and among each other. This leads us to want to connect on a variety of levels and create multiformed relationships, groups and communities in which we not only survive, but live, organise and ultimately thrive.

How Zuckerberg describes the Metaverse is, at its core, a novel response to our basic and fundamental need for social interactions. In that regard, it both disrupts and reaffirms our own humanity.

Indeed, the key objectives underlying the Metaverse aim at enhancing, expanding and to a certain extent, redefining, by means of innovative technologies, the fabric of human networks and daily interactions. The Metaverse is an opportunity to further our journey through new social interconnectedness and to deepen the exploration of what makes us human.

1. The Metaverse: the presence proposition

While we all know the Metaverse is still very much under construction, we are also aware of its promises, which even the best science fiction movies may not have imagined.

Companies currently working on building and developing it~~,~~ have enrolled an army of technological experts at the forefront of innovation, as well as gathered the advice of institutions, bodies and associations that deal with human rights, privacy, security, social inclusiveness etc...~~-~~; they firmly believe that this level of investment across topics, people and sectors is warranted, and even necessary, to unlock the benefits that the Metaverse can offer mankind.

One thing is clear: The Metaverse cannot be built by a single company. There will be a multitude of Metaverses; there will be communities of Metaverses. No single social network, no one brand, will own the Metaverse. Furthermore, traditional concepts of acquiring, sharing, using, and owning one’s space will be transformed in the Metaverse, literally and metaphorically.

A manifest promise of the Metaverse is about breaking down the frontiers of our known reality, whether via mobile internet or our physical body: We will own and use avatars, representations of ourselves or of things by which we want to be represented, through which we will be able to freely move and interact with the surrounding reality to carry out a range of activities under new forms and methods. Eventually, our avatars will become realistic representations of ourselves, faithfully reproducing our gestures, even the most imperceptible ones.

They will reflect our emotions, embody our feelings. They will project the "metaversal" representation of our identity, rendering our natural characteristics and inherent, unfiltered, unconscious behaviours – to reproduce the ways in which we interact in the physical world today, only with many more functionalities.

Reality in the Metaverse will combine elements of "augmented reality" or "AR" with "virtual reality" or "VR". While AR broadly focuses on adding a digital interactive layer on top of the real world, VR focuses on connecting people who are physically apart through immersive experiences. Beyond the definitions however, we can intuitively sense how the Metaverse will transcend the mere sum of its part or mathematical prowesses.

Perhaps the greatest most distinctive feature that the Metaverse promises to deliver, is a deep feeling of presence, which no tech tool has yet provided. This means we will not experience the Metaverse looking at it through the screen of a smartphone held in the palm of our hands; we will be "in" the Metaverse while also being "in" the physical world, thus seamlessly blending realities, or going from one reality to the other. By enabling this, the Metaverse will tear down the barriers resulting from geographical distances on an individual level: We won't need to travel - or even take a single step - to feel in the same space as another person, literally looking each other in the eyes wherever we are located. The fully immersive experiences of the Metaverse will bring people together like no technology has ever allowed.

Turning to the potential applications of the Metaverse, they promise to be both innumerable and boundless. Every sector is in scope: economy and trade, work, social and political life, gaming and entertainment, leisure and travel, education, health, medical processing, the list goes on. In that regard, it has the potential to transform our life even more radically than the internet did 30 years ago.

In terms of human rights and, more specifically, privacy rights and data protection, the implications of the Metaverse will be complex and not always predictable. For lawyers, and~~,~~ in particular privacy lawyers, the novel, unexplored and uncharted scenarios of the Metaverse will present completely new challenges. With AR/VR, the impacts on fundamental rights and freedoms of individuals could also be considered "augmented" and/or lead to situations that we are not yet aware of.

In that regard, it seems necessary to start any reflections with a genuine, humble and candid question: Can our conceptual and technico-juridical categories still function in the Metaverse? And if so, to what extent?

The purpose of this document is to propose some keys to decipher the Metaverse, in light of, mainly, Regulation (EU) 2016/679, known as "GDPR". We will then outline the possible trajectory of our analysis as well as its impacts versus its benefits, from the viewpoint of both enthusiastic optimism and rational realism.

2. The data fabric of the Metaverse

The Metaverse will allow us to experience new realities, composed of data, typically 2D and 3D images and videos, and a host of other layered information that augment and virtualise the physical and imagined realities of people - elements that, in the metaversal landscape, will feel like they magically come to life while flowing avatars interact with each other, running along the surfaces of polygonal models to give renewed shape, meaning and color to our worlds. Such data, images, videos and information will form the fabric of the Metaverse. The difference with our current web environment is that pixels displayed on a screen will be replaced with darting particles, surfacing on a network of immersive environments, digital spaces and realities, and laying the new building blocks of human behaviours towards each other and the world, at both a conscious and unconscious level.

The Metaverse will require an on-going flow of information – both non-personal data and “Personal data”, in the general meaning of art. 4, no. 1) of the GDPR. Among the latter, we need to distinguish between the original data collected, which we will call “human characteristics” i.e. the physical, physiological and behavioural data related to hands, body, face, head or eye tracking data, for example specifications, positions, motions, gaze, and the cc.dd. “Inferred data”, to which paragraphs 2.1 and 2.2 of this report will be dedicated respectively.

The natural corollary of the assumption that the Metaverse will consist entirely of data is that the related data “Processing”, in the terms set out in art. 4, no. 2) of the GDPR, will prove to be a completely inevitable and congenital operation to the very existence of the entire metaversal system. Upon entering the Metaverse, each of our interactions will necessitate a processing of personal data, in real time, from the mere witnessing of the activity of a third party or simple coexistence in a space, to the active collaboration in a work room, partaking in a game or consumption of metaversal goods.

Notwithstanding this, many scenarios and activities in the Metaverse will unlikely fall within the scope of the GDPR.

Quoting art. 2, par. 2, lett. c) of the GDPR, the processing of personal data that is "Carried out by a natural person for the exercise of exclusively personal or domestic activities" is not in scope. Recital 18 also helps the interpreter, clarifying that the GDPR "Does not apply to the processing of personal data carried out by a natural person in the context of activities of an exclusively personal or domestic nature and therefore without a connection with a commercial or professional activity", further specifying that “Personal or domestic activities could include correspondence and mailing lists, or the use of social networks and online activities undertaken as part of such activities"; the recital then adds that, in any case, the GDPR "Applies to data controllers or processors who provide the

means to process personal data in the context of such personal or domestic activities". In light of the foregoing, it therefore seems possible to state, quite definitively, that even in the Metaverse, the GDPR will not apply indiscriminately to all those relationships between private individuals, which are devoid of a connection with the commercial and professional sphere, without prejudice to its applicability to the providers of metaversal services and infrastructure. Beyond the boundaries of the material scope of the GDPR, there is however an “extra-privacy” dimension where the processing of personal data is governed exclusively by the rules of common sense, morality, ethics and normal civil coexistence, as well as the regulatory provisions of other branches of law (e.g. family law, the right to privacy in the traditional sense, the rights to one’s identity, one’s image, one’s dignity and reputation, etc...).

Turning now to the processing of personal data in the Metaverse where the GDPR will indeed be applicable, we want to start by stating that any legal analysis proposed in the following pages does not purport to provide answers, but rather aims at stimulating new reflections, formulating some of the most important questions, and suggesting directional recommendations of the Metaverse needs in relation to the processing of personal data.

2.1. What is the nature of human characteristics’ data?

While no one disputes the fact that the Metaverse will need to operate with information and personal data, we intuitively regard the data required for the Metaverse as being capable of revealing the most intrinsic, innate and distinctive features relating to human characteristics. The processing of these human characteristics, meaning physical, physiological and behavioural characteristics like human actions, gestures, movements and jolts, which can be involuntary and instinctive, will likely lead to the identification of an individual. Furthermore, human characteristics represent the inexhaustible fuel which the Metaverse will draw on to function effectively and thus vibrate with vitality.

At this point, it is necessary to ask whether, by virtue of their structural features, human characteristics constitute mere personal data i.e. a subset of personal data like individual contact details, or another category of personal data like "Biometric data" in the terms set out in art. 4, no. 14) and article 9 of the GDPR.

Biometric data is defined under GDPR as "Personal data obtained from a specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person that allow or confirm their unique identification"; examples are given under art. 4 of the GDPR, i.e. facial images and fingerprint data. Article 9 of the GDPR further refers to biometric data as “Special categories of data” for the purpose of uniquely identifying a natural person. The European Data Protection Committee (better known as "EDPB", an acronym for European Data Protection Board) provides 3 criteria that must be considered in relation to biometric data as special categories of data in its

Guidelines 3/2019 on the processing of personal data through video devices, via an interesting and general digression on biometric data:

1) "the nature of the data": this must be information concerning the raw physical, physiological or behavioural characteristics of a natural person;
2) "the means and methods of processing": the data must result from a specific technical processing, which the EDPB itself describes as a "measurement" of the aforementioned characteristics; and
3) "that allow or confirm their unique identification": the data must be used in order to uniquely identify a natural person, and as such, echoing article 9 of the GDPR ("for the purpose of uniquely identifying a natural person"), and understood as a specific finalistic objective of the processing.

A few important questions should be posed: Firstly, whether article 4 and article 9 should be read separately or rather in conjunction. We believe that one article feeds in, and clarifies, the other and vice-versa. Distinguishing a category like biometric data in the text of the GDPR, and thus making it a separate "sub-category" of personal data, would only seem to make sense if the regulation of this category should be different from that of personal data. It would follow that biometric data should only deserve a specific definition insofar as they are processed differently from other categories of personal data - the GDPR being a tech-neutral regulation, it does not classify data by type of technology applied, but by data sensitivity level, and seemingly only in the case of biometric data, by the purposes sought. Secondly, the three criteria mentioned above are cumulative criteria that apply to the question of how biometric data is to be regulated, based on both its definition and categorisation. An intuitive reading of these criteria in fact point to biometric data being defined and categorised as special categories of data, as they clarify the definition of article 4 and applicability of article 9. In that regard and thirdly, the second criteria on the specific technical processing must be understood as that technology that is specifically developed to technically enable the unique identification of a natural person - i.e. both the condition and the means for that purpose, as opposed to a means to be assessed independently of the specific purpose. In other words, criteria 2 and 3 are intrinsically interlinked. Any technology, including any measurement technology applied to personal data that is not developed for the specific purpose of unique identification, is outside the scope of criterion 2 mentioned above, and therefore irrelevant to the definition of biometric data and its classification as special categories of data. Thus, any measurement technology applied to the physical, physiological or behavioural data is only pertinent to that definition, if and only if, it serves and enables, i.e. "Allows or confirms" the specific purpose of uniquely identifying an individual. The EDPB expressly provides for a reading of both article 4 and article 9 together to make recommendations. One must therefore conclude that, where personal data has not been technically processed in order to specifically result in the unique identification of an individual, it should not be considered as biometric data defined under article 4 and/or regulated under article 9 in the meaning of the GDPR.

As far as human characteristics are concerned, while they are substantially the physical, physiological or behavioural characteristics of a natural person, they are not, by far, systematically processed by specific technical means like measurements that allow or confirm the unique identification, i.e. for the purpose of uniquely identifying a natural person. In the logic of the GDPR, uniquely identifying means tracing with certainty a subject's identity, distinguishing it from the mass of individuals by virtue of characteristics that have been handled, to unequivocally confirm that the said subject really is he or she. The univocal identification occurs when it is determined with absolute certainty that the subject does not identify with any other human being.

Thus, the principle is that human characteristics are not and should not be defined and classified as biometric data and/or special categories of data as per the meaning of the GDPR. While human characteristics can reflect our uniqueness, they are not necessarily used in order to uniquely confirm it.

This reading also has merit of preventing divergent interpretations or lack of consensus among both data subjects, authorities and all stakeholders. It would be rather confusing to distinguish between biometric data based on a few words of the GDPR that may, or may not, clearly indicate the status depending on the circumstances. The most practical and understandable reading of the GDPR should limit biometric data to all of the three criteria mentioned above, and any other human characteristics that do not fulfill the three criteria, should be considered personal data, or "common data" outside any categorisation as non-sensitive or sensitive biometric data.

Furthering this thought, in the Metaverse, artificial intelligence, i.e. "AI" technologies that will power the metaversal scenarios, will be limited to the capturing and processing of human characteristics for the main purpose of enabling the concrete functioning of the Metaverse.

These human characteristics are not generally grasping the essential traits of our unique appearance, being and actions, and they will not normally be used in order to identify us uniquely. They will represent, as mentioned above, the mere indispensable premise for the functional mechanism of the Metaverse, its intrinsic characteristic that will allow us to truly experience "that deep feeling of presence" Mark Zuckerberg talks about and, therefore, in essence, the means to experience metaversal sociability. And even if human characteristics could be used to uniquely identify the data subject, so long as this possibility remains a mere unrealised potential, it would be entirely insufficient and inappropriate to drive a definition or categorisation as biometric data. Thus, for example, when in the virtual coffee shops of the Metaverse, we find ourselves smiling in front of a friend, the Metaverse technologies will reproduce the same facial expressions on the faces of our avatars that, within the same instant, we mimic in the earthly reality. These are reproductions of our very personal ways of appearing and moving, which belong to us and only us, as unique beings; yet such facial expressions will

not be used for the purpose of confirming, or allowing our unique identification, and cannot therefore be considered biometric data in the sense indicated above.

It follows logically that the processing of human characteristics would be able to rely on the legal bases referred to in art. 6 of the GDPR, rather than that of art. 9 of the GDPR.

Human characteristics are thus consecrated in their nature as so-called “common data”, which will undoubtedly ensure greater fluidity and ease in circulation and use.

2.2. How should we consider inferred data?

While human characteristics would not be subject to the processing regime pursuant to art. 9 of the GDPR and are therefore "common data", the same cannot always be affirmed in the case of cc.dd. "inferred data". Inferred data is the information that can derive, and be conceptually elaborated, from human characteristics. This data is the data that a third-party observer could deduce - "infer" - from the analysis of human characteristics or, in other words, interpret from the collection, absorption and rationalisation of human characteristics.

It cannot be reasonably excluded that this inferred data may fall into the special categories of data pursuant to art. 9 of the GDPR. In this regard, the Metaverse will offer a very high degree of accessibility to anyone, including the disabled, allowing them, through the virtualisation of reality, to experience the metaverse without the limits that they might experience in their everyday physical reality. By processing the human characteristics of these categories of people, it will be inevitable to deduce sensitive information concerning, for example, their health status. In principle, health data falls within the scope of art. 9 of the GDPR, and the legal consequences in terms of processing and circulation of the same will apply.

What should be emphasized however is the fact that whilst data inferred could belong to the special categories of data referred to in art. 9 of the GDPR, it will and should in no way compromise the nature and classification of human characteristics as common data. Human characteristics and any potentially inferred data, even though interdependent, are not superimposable, interchangeable or “fungible” concepts. These remain two autonomous, distinct legal categories. The processing of these two types of data takes place on the basis of two autonomous and distinct assumptions of legitimacy.

2.3. How to legitimise personal data processing in the Metaverse?

Having examined the issues related to the nature of human characteristics and inferred data, we will now share some observations regarding the legitimacy of the processing of this data in the Metaverse - a matter that poses new questions considering the dynamic, seamless and real time processing activities that will unfold in the Metaverse. To jurists engaged in identifying the most appropriate legal basis for the processing of personal data pursuant to Articles 6 and 9 of the GDPR, the objective will be to adapt the regulatory letter to the metaversal reality in the most constructive manner, one that both protects individuals and enables innovation. It will be an exciting challenge, perhaps even more so than other challenges to date, as the metaverse promises to improve the ways in which we humans interact with each other and the world. It is certainly keeping with the historical dialectic on the application of legal norms, whereby on the one hand, the law seeks to be "tech-neutral" and principle~~s~~-based to anticipate future trends and emerging technologies, and on the other, the evolving and even relentless technological advancements always tend to stay several steps ahead of the law, initiating new cycles of regulatory debates that often end up being momentarily solved through the addition of new laws.

In that sense, it will be necessary, for example, to meditate on the conceptual category of consent as a legal basis for the processing of personal data, on the methods of data collection by the data controllers, as well as the "needs-basis" in metaversal scenarios.

Pursuant to art. 4, no. 11) of the GDPR, consent is defined as any manifestation of the free, specific, informed and unambiguous will of the data subject expressed via means of an unequivocal positive declaration or action. The EDPB's Guidelines 5/2020 on consent pursuant to Regulation (EU) 2016/679 requires that the most effective and rigorous method of collecting consent be considered, including from the perspective of the accountability requirements. We've seen various consent practices carried out by controllers, either validated or rejected by the competent authorities; think, for example, of the practices around consent for the processing of cookies. A minimum common denominator between the various forms of consent lies in the existence of an active and unequivocal externalization, through both express declarations and conclusive behaviors that denote an adequate coefficient of awareness and positive will from the data subject.

The dynamism inherent to the functioning of metaversal relationships and the instantaneity of the processing activities are disruptive by nature and will inevitably require an adaptation of the traditional methods of acquiring consent. While it should not mean giving up the active and unequivocal character that legally characterises consent pursuant to the GDPR, it is also indubitable that it will be necessary to explore and find new and more agile forms of conscious self-determination of the data subjects in the Metaverse. In this context, raising the awareness of all stakeholders, controllers, data subjects and other relevant

parties will be central to the debates, even more so than today, as we shift from viewing clusters of colored pixels arranged on the screen of a smartphone or a PC, to incarnating avatars capable of moving in real time within a three-dimensional space. As part of raising the awareness of data subjects with regards to their privacy rights in the Metaverse, ensuring that they are also accountable for their own behaviour, and how this accountability should look like in the Metaverse, are important aspects of the debates.

In any case, consent cannot be considered as the sole appropriate basis for the processing of personal data in the Metaverse, in particular in relation to its functioning and the interactions that will take place. Art. 6 of the GDPR poses other conditions of lawfulness, that in principle, would fit the logic of metaversal processing: specifically, art. 6, par. 1, lett. b) of the GDPR, whereby the processing is lawful, insofar as it is necessary for the execution of a contract, which the relevant data subject is a party to, or for the execution of pre-contractual measures requested by the data subject.

In that sense, we must free ourselves from any potential general perception around the inevitability of the requirement of prior specific consent for the processing of personal data in the Metaverse. The reality is that very often, the processing will result from the needs or desires of the interested parties i.e. to play a 3D game, meet colleagues in virtual work rooms, socialise in a virtual coffee place, or just hang out in their own spaces to exercise or immerse in a virtual travel experience. To execute these needs and expectations of metaverse users, an agreement on the terms will be necessary, and thus the logic underlying art. 6, par. 1, lett. b) of the GDPR would be the best fit. This will require interpretation of art. 6, par. 1, lett. b) of the GDPR from a needs-basis perspective, while a consent-based approach will be on a case-by-case basis to effect applicable legislation.

3. Augmented impacts: framing secondary uses and data sharing in the Metaverse

The virtual and augmented reality of the Metaverse will likely mean increased impact on the rights and freedoms of the data subjects. In the Metaverse, personal data will need to flow on an on-going and real-time basis. Attempts to unjustifiably prevent or limit the circulation of data that will animate the Metaverse would mean emptying the Metaverse of meaning and opportunity, depriving it of its essence and compromising its mission, which is to interconnect individuals in new realities.

These dynamics can give a renewed meaning to the concepts of “Communication”, “Making available” or “Dissemination” of personal data, and the wider logic of the GDPR, art. 4, no. 2). Data processing in the Metaverse could take on a systematic and persistent character, which could materialise in continuous data flows indispensable for the very functioning of the Metaverse. By

incarnating through our avatars into the Metaverse, we will disclose certain human characteristics to our interlocutors, in real time and in new, and interoperable worlds.

Having said that, it will be something very similar to what happens in real life; yet, with a difference: In the Metaverse, “avatarising” oneself will take place through the mediation of virtualising technologies that will convert the images and forms of our being and our acting into new types of personal data. Hence, the applicability of the GDPR and its protections for all data subjects.

Among the potential impacts referred to above are the secondary uses of personal data. With this expression, we usually allude to the cases in which a subject, in the capacity as data controller, has collected and processed data for a specific purpose - defined as an "original" purpose and known as the "primary use" – and who subsequently intends to process the same data for a further and additional purpose i.e. a "new" purpose, the cd. "Secondary use". Among the secondary uses, there is also the cd. "Further processing" (art. 6, par. 4 of the GDPR), which occurs specifically when the data controller intends to further process on the same legal basis as that which he relied upon when collecting and processing the data for the original purpose.

The secondary uses and further processing will be focal points due to the processing dynamics in the Metaverse and will require that privacy experts study strategic ways of conceiving these particular types of processing and address the new legal problems connected to them.

Inevitably, while there will be increased vulnerability risks as a result, this will not necessarily mean increased defenselessness. Companies and professionals working on the Metaverse will have to put people’s privacy at the center of their preoccupations, and leverage the fundamental principle of data protection by design sculpted by art. 25, par. 1 of the GDPR. The Metaverse can only really work and garner social acceptability, if and when, maximum respect for the fundamental rights of the data subjects is guaranteed through suitable, solid and effective tools and protection mechanisms capable of governing and regulating, among other things, the phenomena of on-going circulation of data and secondary uses.

In addition to the implementation of the principle of privacy by design, there is another essential condition for the safe functioning of the Metaverse: that is, compliance with the principle of privacy by default, provided for by the same art. 25 of the GDPR in paragraph 2. By virtue of this principle, the data controller is obliged to carefully examine a series of specific parameters, such as the quantity of personal data collected, the scope of the processing, the retention period and the accessibility to the data themselves, and consequently implement adequate technical and organisational measures, so that the personal data processed by default are exclusively those necessary for the specific processing purposes pursued. In particular, as specified in the last sentence of the aforementioned art.

25, par. 2 of the GDPR, the privacy by default principle requires data controllers to ensure that the personal data processed are not made accessible to an indefinite number of natural persons without the prior "intervention" of the data subject. The principle of privacy by default, in fact, directly attributes to the data subject the right to regulate the use of his or her data~~,~~ before the processing begins~~,~~ via the settings' configuration, relating for example, to data sharing (i.e. which data to make available to third parties and under which conditions), thus indirectly governing information flows.

Because in the Metaverse the free flow of data on human characteristics will represent the indispensable premise of metaversal sociability, one of the challenges will be to ensure that data subjects can easily adjust and graduate the settings on the sharing of their human characteristics without unduly compromising the core functioning of the Metaverse. It will be necessary to seek and achieve a reasonable balance between the logic of the free flow of human characteristics and the obligation to ensure compliance with the principle of privacy by default. In other words, the guarantee of an appropriate privacy by default policy must also be compatible with the needs of the Metaverse. As human beings, we are designed to communicate and interconnect with one another. This "core feature" is as important as the protection of our data and privacy.

To take a light-hearted example of this, let's imagine a gallant and romantic encounter in the Metaverse: preventing the expression of any feelings like shyness or joy through the privacy settings could distort and compromise the development of the relationship. Same for a job interview in the Metaverse: How could a recruiter really understand what kind of professional person we are, or our strengths and weaknesses, if we do not allow for the disclosure of our human characteristics? Without the processing of human characteristics, the Metaverse would be deprived of most of its meaningful use cases.

4. Augmented rights: unlocking the value of the Metaverse

In the same way that impacts will be "augmented" in the Metaverse, human rights, privacy and data protection will also be "augmented".

Taking a step back to the genesis of privacy, it can be said that it was born from the "*ius excludendi alios*" principle, or right to be left alone or not intruded upon. In other words, the right to confidentiality or anonymity in an eminently introverted, negative and passive conceptual configuration. It then progressively asserted itself as the right to protection of personal data, which grants data subjects the power to consciously govern the flow of data concerning them and~~,~~ the rights to information and self-determination, thus shifting the configuration to an extroverted, positive and active dimension like the one we have today.

Tomorrow, in the Metaverse, the concept of privacy will most certainly again evolve: It will mean redefining metaversal freedoms, metaversal rights and self-determination, metaversal identities in neo-relational, social and identity ecosystems. This conceptual evolution will require a new way of understanding and enhancing the principles of privacy by design and privacy by default pursuant to art. 25 of the GDPR.

We need to brainstorm on new methodological approaches for carrying out data protection impact assessments, also known as “DPIAs”. These are accountability exercises defined pursuant to art. 35 of the GDPR, which require an in-depth evaluation of the risk profiles associated with processing, and implementation of methods and safeguards capable of containing the impact on individual rights and freedoms. In the future of the Metaverse, DPIAs will need to encompass impact assessments in relation to the protection of our avatars within the Metaverse, meaning that they will no longer be limited to “human data subjects” but extended to the “metaversal person”.

Moreover, we should keep in mind that a legal reasoning that hinges only on privacy and on the logic of the legitimacy bases provided for by Articles 6 and 9 of the GDPR runs the inexorable risk of being incomplete, inflexible, short-sighted and inadaptive. The right to privacy and protection of personal data is solemnly sanctioned by international charters and treaties, but it coexists with other fundamental rights, such as constitutionally guaranteed and equally consecrated rights at national and international level. This is a completely natural and physiological coexistence, a dialectic immanent in all modern constitutional systems, and intimately connected to the same axiological matrix of fundamental rights, each of which consecrates and recognizes juridical relevance of competing interests equally worthy of protection. We refer, for example, to the freedoms of expression, opinion and thought, including political, philosophical and religious expression.

It is thus imperative to raise one's gaze beyond Articles 6 and 9 of the GDPR, and focus on the other fundamental rights that coexist with the right to privacy and data protection. This “extra-privacy” perspective may represent, in the Metaverse, an oxygen valve of essential importance for privacy experts, intent on seeking the basis of legitimacy of the processing in the interpretative meshes of Articles 6 and 9 of the GDPR, and the recommendations of the competent authorities. It will be necessary to carefully weigh in all the elements at stake, to balance the guarantees of the least possible sacrifice to the right to privacy and the protection of personal data with the promotion of other equally important rights.

And indeed, the Metaverse will provide new opportunities to “augment” many other human rights. Some of us can take for granted having two arms, two legs; or travelling on long-distance journeys; or living where our loved ones also live. This is far from the case for everyone.

The Metaverse is set to provide more equal opportunities and rights for human beings: Those who cannot walk will be able to do so through their avatar in the virtual streets of the Metaverse; those who do not have the opportunity to travel and discover new places will be able to do so at any time by exploring the virtual horizons of the Metaverse; those who are separated by long distances from those they love will be able to experience “that deep feeling of presence” promised by Mark Zuckerberg and enjoy a true and warm embrace in virtual reality. The Metaverse aims at making these dreams and needs come true.

And it does not stop there. The Metaverse will offer new opportunities with regard to the entrepreneurial, marketing and economic spheres: The circulation of goods and services in the Metaverse and across Metaverses will be “augmented”, and as such foster healthy competition for all. Politics too, will change both in form and substance by allowing candidates and leaders to get closer to citizens – in the same virtual space indeed. We have already seen an example of this during the South Korean presidential election.

From this angle, the Metaverse will represent the source of new boundless opportunities for those hindered in real life and will create new accessibility, rights, inclusiveness and reduce discrimination. The Metaverse will allow for new ways of working, doing business and exercising one's freedom of economic initiative, as well as new forms of political and institutional dialogue. For all these reasons, we want and need to strongly affirm the critical necessity of adopting a balanced and consciously optimistic approach to risks, benefits and safeguards in the Metaverse. We must avoid irrational skepticism or illogical mistrust.

Let’s now conclude on the very choice of the word "Metaverse", which is not accidental: In addition to evoking an undoubted assonance with the term "universe", which is very effective from a marketing perspective, it also contains profound and fascinating etymological values:

1. the prefix "Meta-", which comes from the ancient Greek "*mèta*" ("μετά"), originally meant "with" or "after", and expressed the idea of a succession or posteriority before acquiring the value of "trans" in today’s modern age to designate what lies beyond the boundaries of a given matter (for example, metaphysics is the science that studies what transcends the dimension of natural things);
1. the suffix "-verse", which derives etymologically from the Latin "*versus*", past participle of "*vertere*", means "to turn" or the "direction to which the motion is directed".

From the combination of the two linguistic segments, we can state that the term "Metaverse" indicates "what goes beyond" and, in particular, what goes beyond our current universe, world, reality. The Metaverse expresses the idea of both a path to take, and a destination to reach i.e. a new world with new opportunities, new rights and new freedoms.

5. Final considerations: market-led approach and technological progress

As we witness the Metaverse slowly and gradually unfolding before us as a new virtual world, bringing to life a continuous flow of information and images, including personal data such as human characteristics and inferred data, we will keep reflecting and asking many questions regarding its implementation, functioning and role in our everyday life, particularly from the perspective of the possible impact to our rights and freedoms. With regard to the protection of personal data, we have attempted to describe some of the key questions surrounding the applicability of certain conceptual categories provided for by the GDPR, and how some of its principles and safeguards could be implemented.

In addition to the regulatory and legal analysis and solution-building, we should also mention the merit in fostering the development of industry standards by letting the market and its competitive dynamics produce the rules, technological practices and codes of conduct that are necessary and appropriate to modulate the novel and peculiar dynamics of the Metaverse. This approach will be particularly relevant since the Metaverse will not be the product of one single social platform or major tech brand, but will configure a new complex ecosystem of a variety of small, medium and large players from different sectors, which will be called to operate and collaborate with each other. To that extent, the most adequate guarantees and forms of protection for the rights and freedoms of the interested parties may well indeed develop from within the market, as a result of its competitive synergies that will shape, even perhaps through some necessary trial and error, the key policies–destined to gradually settle into the general practice.

Notwithstanding the fact that there are still many unanswered questions, we should feel enthusiastic about wanting to experience the Metaverse and the possibilities it can offer to increase our rights and opportunities for the benefit of all. We should look to the future of the Metaverse with positive excitement, as well as rational clarity.

And finally, having presented our reflections in the preceding pages, let’s now return to the question formulated at the beginning of this paper, when asked about what Martian scholars and intellectuals would understand about us, from their faraway future, with only two pieces of information at their disposal, i.e. the Book I of Aristotle's Politics and Mark Zuckerberg's audiovisual presentation of the Metaverse at the “Connect2021” event.

We still have the same answer: The most significant conclusion they would draw is that man is a social animal, driven by an innate instinct to communicate, share and interconnect with one another through work collaborations, business ventures, exchanging ideas and thoughts, evolving cultures, co-creating and sharing moments of excitement and love.

If being social indeed represents our most natural functional destination, our most authentic teleological inclination, then man is also an "animal", from the Latin "animal", derived from "soul", which expresses the idea of a vital principle, a breath of life. "Anemos" in Latin carries the idea of a wind, of a dynamic and industrious movement, as opposed to inertia, which is so close to death. We can thus deduce that the main tool for being and becoming who we really are - social animals - is that, which will enable a perpetual flow of vibrant social interactions, like what progress and, in particular, technological progress provides.

Technological evolution represents the universal language of humanity, it belongs to its millenary history, it represents its genetic makeup.

There is nothing more human than technology, from the wheel and the concrete to the steam trains and the electric cars, and later the computer-the internet and tomorrow, the Metaverse, which, in giving shape to a new horizon of human technological progress, will be nothing more than another testimony of the evolution of human civilisation, and another tool at our disposal to further our human destiny.