Journal of Ethics and Legal Technologies – Volume 3(2) – November 2021

Surveillance And Profiling. Online Person's Privacy Between Criminogenic Structures And Legal Paternalism

Enrico Maestri

Department of Law
University of Ferrara

Abstract – Cyberspace is an ambivalent place, where many activities overlap with real world ones and many others are peculiar to it, revealing its plasticity. The pace of technological innovation is still growing, together with new insidious forms of invasion of people's private lives. There is still a strong temptation for us to waive our rights in order to enjoy the technological paradise we are offered. A new entity—the digital person—has made its appearance in the digital ecosystem, as a technological outcome of the reconfiguration of the classical concept of person. Our privacy is being progressively eroded away as a result of our increasing acquiescence, apathy and unconcern and our explicit support for measures sold to us as necessary and harmless. Though it is still too early to say that privacy is almost dead, new generations, whether they like it or not, are playing a leading role in a cultural praxis and in a primary socialization which are remote from the concept of privacy. The purpose of this paper is to discuss and investigate whether or not it is still possible to introduce new effective forms of governance designed to defend children as digital persons: their rights to dignity, habeas data and personal data privacy.

Keywords: Cyberspace, Inforg, Code, Personal data protection, Digital person, Privacy

1. Introduction

There is no doubt that cyberspace and the composition of the related forms of post-organic life will very soon be the central focus of intense speculation and bitter clashes and debates, above all if we consider that not only large multinationals, but also research and development institutes, university departments and individual researchers are currently engaged in discussion and involved in engineering the ontological and normative framework of cyberspace. Every day, 3.3 billion searches are conducted on 30,000 billion pages indexed by Google; over 350 million photos are shared, and 4.5 billion likes expressed on Facebook; 3 billion digital citizens exchange 144 billion emails. We generate this volume of information in two days[1].

People are by now the digital inhabitants of the Web: they express themselves anonymously, but at the same time they have a profile and are constantly seeking to optimise it. The Web forces them into a form of self-illumination that reduces the distance between public and private. Digital media such as blogs, Tik Tok, Twitter, Facebook and Instagram de-mediate communication: subject and object become confused, everyone exploits themselves, each person produces and disseminates information, so there is a continual tension between exhibitionism and forms of intimacy, a perpetual intertwining between online spaces and offline spaces within an overall framework whose practices, representations and consequences are to be found (mediated or not mediated) in reality. People live a "dual realm", online and offline[2], that is, a state marked by a sort of *digital promiscuity* where experimentation with relationships produces a digital neighbourhood without the need for relational depth. The limits of the new digital media make people not only seem a bit colder, irascible and intolerant: online it is easy to be really less inclined to behave in a civilised, courteous manner, at

[1] Cardon 2016, 7 ff.

[2] I wish to highlight that this dual realm in which a person expresses his personality does not consist in two equitable worlds. According to Niklas Luhmann, the offline environment allows an individual to express values and choices of action with a high coefficient of differentiation. Here, i.e. in the offline ecosystem, all experiences and all actions can only present themselves as highly contingent systems of action. In the former case, one can speak of experience, in the latter case of action. In contrast, the online environment is a cybernetic communication system. The notion of action is uncoupled from the bio-psychological support of the individual and attributed to the self-referential social system. People, reduced to units to be used by systems, matter less than actions, understood as decision points (information) through which systemic communication networks structure themselves.

There, i.e. in the online ecosystem, a binary logic prevails, so that preferences and problems with a selective character are structured in a form such that what is already given is always paired with a corresponding alternative. Unlike the world of atoms, society is a place, has a territory inhabited by bodies that can decide on different courses of action, being able to obey or disobey the rules.

least to the extent demanded by social norms. Therefore, a loss of innocence goes hand in hand with the expansion of a network.

Interfacing with a machine can amplify an amoral indifference towards human relations. Cyberspace renders the present denser; it represents a deep, structured space that can be materially inhabited and produces a sensation of purely spectacular physical freedom, in the sense of freedom *from* one's body, and in particular from the sensation of loss of control that accompanies the growth of teenagers and causes dizziness.

This "space without place and without bodies" is emphasised by the metric reputation systems that drive the online calculator, so that internauts can measure themselves on their own. Every click is recorded and used to generate performance and predictive feedback that incentivizes further actions eliminating the boundary between privacy and surveillance, between self-illumination and reputation. If, therefore, a person becomes a flow information that is continuously exchanged in a *coded* system composed of a "data wall", how is it possible to discern that individual's identity in such a chaotic context, where no entity is well defined, and the only identifiable element is digitised information?

Concepts such as integrity, dignity, action, thought or truth belong to the Earth's *nomos*; the *digital turn* has made it problematic to safeguard these values, as each person becomes an ethereal entity that is not constant over time and space, with individual characteristics enabling them to be distinguished from other biological or artificial entities operating in the Web.

A person loses every re-putation (every ontological thinkability) and becomes an informational organism destined to mutate in every instant[3]: their configuration makes it virtually impossible for an institutional entity aiming to protect the *digital person*, to reconstruct that person's identity and establish whether an injury to their *reputability* has occurred.

[3] Contrary to what was affirmed by Floridi, I argue that digital persons are not only informational objects (and moral patients) living and acting onlife: people do not become inforgs because in a by now near future they will live mainly online in the infosphere. If we were to accept this argument, we would end up repeating Descartes' error whereby the informational side—res cogitans—guides (like a spectre in a machine) the biological matter—res extensa—of human beings. In Floridi's neo-modernist approach we see an obscuration of the human body. If we want to understand the social phenomenology of digital persons we need to define the environment in which they act and understand what happens to the human body, that is, understand beforehand how digital persons are constructed. In short, what we need is an epistemic process contrary to the one elaborated by Floridi: it is not a matter of reontologising the world and human beings that inhabit the infosphere, but rather to radically deontologise the digital person in order to avoid an infocratic drift of cyberspace. See L. Floridi, La quarta rivoluzione. Come l'infosfera sta trasformando il mondo, Milan, 2017.

On the basis of these reflections, in this essay I intend to examine and discuss the following argument:

cyberspace is an ambivalent technological and communication system, where many activities overlap with real-world activities and many activities are specific to it, revealing its plasticity. The pace of technological innovation continues to grow and is accompanied by new insidious forms of invasion of people's private lives. There is a strong temptation for us to waive our rights in order to enjoy the technological paradise we are offered. A new entity—the *digital person*—has made its appearance in the digital ecosystem, as a technological outcome of the reconfiguration of the classical concept of person.

The development of computing applications enables a connection between people and their corresponding digital identities: individuals who form links without spatial constraints or the need for a shared physical presence become part of a digital "swarm". Our privacy is being progressively eroded by our increasing acquiescence, apathy and indifference or explicit support for measures that are sold to us as necessary or innocuous. Though it is still too early to affirm that privacy is dead, digital persons, whether they like it or not, are playing a leading role in a cultural praxis and in a primary socialization which are remote from the concept of privacy (paragraph 2).

The new General Data Protection Regulation (Regulation EU 2016/679, entered into force on 25 May 2018, without requiring any transposition procedure) makes repeated reference to the importance of protecting the personal data of children. I feel that the regulation of this specific area is a paradigmatic representation of the tendency to *contractualize* the availability of personal data with counterparties that operate in the digital market (as in the case of first-party cookies and third-party cookies). In practice this European regulation (hereinafter GDPR) has not shown to be capable of adequately harmonising the rules related to them and, therefore, substantial restrictions are established by pre-existing or new laws or codes of conduct at a national level.

The GDPR has been considered a Copernican revolution in the area of personal data protection. However, attention should be paid to the difference between the concepts of data protection and privacy (a term never used by the European legislator, except in a note), as the relationship between them is not immediately clear. The two aspects overlap, so much so that the latter is usually invoked as an interest supported by the former. More often, however, personal data protection is confused with privacy protection: they are complementary notions, not synonyms. The collection, use, storage or transfer of personal data does not always imply a violation of privacy. Indeed, the notion of personal data is so broad as to include information that is not necessarily private. The idea that I will put forth is that the personal data protection regulation was not constructed in such a way as to enable complete protection of individual privacy. I will attempt to support this idea by using the argument of "children as digital persons" (paragraph 3).

The *code* (or *Lex informatica*), i.e. the software and hardware making up the cyberspace, imposes a normative framework (*codification*) of individual and collective online behaviour. This does not mean denying the regulatory function of the law on cyberspace; we need only consider, for example, the penalties provided for by copyright laws, contract law and laws regarding defamation and obscenity. However, cyberspace is an architectural system that implements the *codifying* of human normative spaces, i.e. the channelling of modes of action, of the logical and functional governance of cognitive processes, of possible motivations and practicable or available alternatives. The *code* is performative and predictive: "it does what it says and it imposes what it predicts (*tertium non datur*)" (paragraph 4);

In my conclusion to this essay, I will consider the question as to whether we can still find room for effective forms of governance to protect the digital person: their right to dignity, *habeas data*, *habeas corpus* and the confidentiality of personal data on the Internet (paragraph 5).

2. The digital person

The setting of one of Dave Eggers' latest novels, *The Circle*, is the campus of a large company (the *Circle*). The young protagonist, Mae Holland, is and remains alone, without any prospect of collective action and class solidarity. The mission of the company (which does not produce material goods), is to connect the largest number of people possible, but at the same time to render them transparent, induce them to give up every form of privacy. In a dystopic future, everyone will move around wearing a series of devices that will make them visible and exposed to tens of millions of other individuals. As she aspires to become part of the elite community of the *Circle*, Mae Holland does not hesitate to give up her privacy for a regime of absolute transparency, which requires her to share every personal experience over the Internet and broadcast her life via live streaming. Everything is perfect inside the *Circle*: the best people have created the best systems and the best systems have created the most beautiful place in the world. However, in order to be able to enjoy the conveniences offered by the *Circle*, people have to completely give up their privacy.

Individuals become a goldmine from which to extract the valuable information they hold within them: by giving up their data voluntarily, they play an active role in destroying their own privacy.

If personal data is transformed into a commodity, it is clear that from the moment it goes online the rights recognised in the real world become more fragile and blurred. They are subjected to the pressure of supranational private actors which, in order to get around certain legal constraints, choose the most advantageous jurisdiction for the purpose of *forum shopping* in the regulatory space. An ideal habitat for anyone who wishes to exercise global surveillance over *digital bodies*[4] is created by the combination of this legal capacity with the digital data-gathering capacity offered by the rapid development of information technologies, the extensive spread of the Internet and, finally, the creation of *Big Data*[5]. It is analysed and managed with the data mining process, i.e. with a set of techniques (data collection, application of algorithms, examination and interpretation of results and application of profiles) which, based on the data collected, generate new information (so-called "inferred data") used to predict outcomes before they occur[6].

Lastly, attention is focused on the possibility of applying automatic learning methods to large volumes of data by providing machines with a way to learn and derive the necessary information for carrying out their tasks from the data they collect: this process is defined as machine learning[7].

Machine learning undeniably has great potential. It overcomes the problem of information overloads, generates new solutions and offers information and consulting services. Moreover, it can help to tackle the great challenges facing us today in the field of medicine and at a socioeconomic level. However, concerns have arisen about possible violations of fundamental individual and collective rights, in particular the respect for privacy and democracy.

Machine learning feeds on characteristic individual or social behaviours and personal data, giving rise to a spiral of feedback that creates huge datasets: what we define as big data. Analytics Big data—but in general

[4] Lyon 2002, 138-141.

[5] Regarding the impact of big data in contemporary society, cf. Mayer-Shönberger and Cukier, 2013.

[6] Zarsky, 2011, 285-330.

[7] Within artificial intelligence (AI) and machine learning, there are two basic approaches: supervised learning and unsupervised learning. The main difference is one uses labeled data to help predict outcomes, while the other does not. However, there are some nuances between the two approaches, and key areas in which one outperforms the other.

Supervised learning is a machine learning approach that's defined by its use of labeled datasets. These datasets are designed to train or "supervise" algorithms into classifying data or predicting outcomes accurately. Using labeled inputs and outputs, the model can measure its accuracy and learn over time.

Unsupervised learning uses machine learning algorithms to analyze and cluster unlabeled data sets. These algorithms discover hidden patterns in data without the need for human intervention (hence, they are "unsupervised").

all the algorithms connected to machine learning—lacks transparency, as automatic learning does not provide explanations regarding the decisions it produces[8]. An information gap ensues, since the person on the receiving end will not have any means to challenge the decision resulting from the algorithm. Transparency should be guaranteed, however, also in relation to micro-decisions, which, taken together, could become important and impact an individual's rights. Latest generation information systems are comparable to black boxes: nothing can be known about their operation or the process leading to decisions that—without an explanation—are unchallengeable.[9]

Personal data can no longer be identified with details such as name, address, marital status etc.: it embraces any *biographical information* regarding an individual, namely all the information describing a biological, economic, social or financial element of a person. Every data transaction taking place over the Internet is stored in big data in order later to be analysed and defragmented by the service provider or by a third-party firm, which acquires the data in the marketplace. Inferred data (which does not fit the definition of personal data or metadata) will be stored and remain forever part of the big data, thus definitively eluding the control of its legitimate owner, i.e. the individual it refers to.

The profiling process renders every individual's life transparent, exposing them to the extremely minute, hyper-technical control of power[10]. Consequently, there arises a need to protect the rights of a new entity—the *digital person*—who moves about in cyberspace, where temporal and

[8] Big data and machine learning aren't competing concepts or mutually exclusive. To the contrary, when combined, they provide the opportunity to achieve some incredible results. In fact, successfully dealing with all the V's of big data helps make machine learning models more accurate and powerful. Effective big data management approaches improve machine learning by giving analytics teams the large quantities of high-quality, relevant data needed to successfully build those models. Many organizations have already discovered the power of big data analytics enhanced by machine learning. For example, Netflix uses machine learning algorithms to better understand the viewing preferences of individual users and then provide better recommendations, helping to keep people on its streaming platform for longer. Similarly, Google uses machine learning to provide users with a more personalized experience, not only for search but also to build predictive text into emails and give optimized directions to Google Maps users.

[9] Most algorithms in the world today are created and managed by for-profit companies, and many businesses regard their algorithms as highly valuable forms of intellectual property that must remain in a "black box". Some lawmakers have proposed a compromise, suggesting that the source code be revealed to regulators or auditors in the event of a serious problem, and this adjudicator will assure consumers that the process is fair. This approach merely shifts the burden of belief from the algorithm itself to the regulators. This may a palatable solution in many arenas: for example, few of us fully understand financial markets, so we trust the SEC to take on oversight. But in a world where decisions large and small, personal and societal, are being handed over to algorithms, this becomes less acceptable.

[10] Foucault 2014, 214-247.

spatial limits no longer apply[11], and whoever possesses the most complete knowledge, and the best technological means will dominate. Today, networks and computers do a great deal more than supplant the meaning of human thought. They do not limit themselves to emulating intellectual processes and our repeatable programs; they also have the effect of discouraging more complex mental procedures[12].

The *digital person* travels continuously between two worlds interconnected by platforms, veritable vehicles of transmission, memorisation and manipulation of every piece of information; this global digital *nonplace*[13] is the World Wide Web, a technology which, starting from 1991, has profoundly modified the worldview of contemporary man, as well as transforming his everyday habits and customs.

In this environment, where barriers have been broken down and rules do not seem to exist, users feel like they are players in a large virtual game where everything is allowed: they need not worry about the social or legal consequences of their *digital actions.*

Cyberspace is essentially a made-up world; being a world it requires an architecture (World 3 as described by Popper), physical objects (Popper's World 1), subjects and objects, processes and an ecology; being made-up, an incarnate fantasy (Popper's World 2) erected upon a fundamental representation of our imagination, it enables us to direct data flows into different spaces: our ego is multiplied, physics becomes variable and perception becomes extendable[14].

A real person and an artificial intelligence (*informational organism* or *inforg*[15]) cannot be considered to lie on the same plane, though both act in a digital environment. From a technical viewpoint, the comparison holds up perfectly because—as Luciano Floridi argues—it does not matter whether information comes from a living being or an artificial entity[16]. However, by

[11] Lyon 2002.

[12] Rushkoff 2012, 14.

[13] The neologism non-place was introduced by Marc Augé and defines two complementary but distinct concepts: on the one hand, spaces created for a specific purpose (usually transportation, transit and commerce) and on the other hand the relationship that forms between individuals and those same spaces. See Augé, 2009.

[14] Popper 2012.

[15] Floridi 2012.

[16] In Floridi's view, people can be defined as inforgs, where this term means a new subjectivity constantly connected in the Internet. In The Onlife Manifesto, Floridi affirms that the distinction between online and everyday experience is becoming increasingly faint, to the extent that it will eventually disappear altogether. The here (analogue, offline) and there (digital, online) will become definitively fused in favour of online life: life is translated online and human society becomes onlife. Floridi uses this expression to indicate how online experience and offline life blend together, so the distinction between real and virtual

adhering to this viewpoint we risk losing sight of the distinctive attributes of humans, such as the value of dignity and the moral sense of belonging to one's own species.

The *digital person* is made up of all the information an individual enters into the Web: every action stored in files (digital traces left by their navigation and documents produced through interaction with the web environment they find themselves in) represents the legal-cybernetic personality of any individual expressed in the *nonplace* which is the Internet and forms part of their digital identity[17].

Digital identity is something that is in the virtual dimension and does not directly interact with us, people, but interacts only with machines. Digital persona on the other hand, is what people use, to make sense of interactions in virtual space.

The panoply of digital innovations and the massive use of 'smart' technologies have transformed the person (in the classic sense of subjective identity and psychological and physical integrity) into a *digital person*, i.e. into a cluster of data[18] in which corporeality, instead of disappearing, is *socially* relocated and *technologically* governed.

In this respect, the principle of *habeas corpus* upheld in World 1 is not obscured or superseded by the principle of *habeas data* recognised under the World 3 architecture as a form of protection of the digital person, on condition, however, that the advent of cyberspace is conceived as a new stage towards the *concrete realisation* of the world we dream and think about, a world of abstractions, memory and knowledge.

Both in the real world and in the digital world, people recognise themselves through their recollections, experiences and interests, i.e. through the fragments of memory contributing to the creation of a self-image and personal biography[19], made up in turn of all the files (photos, videos, documents), all the information and actions produced by people during the time spent online: that is to say, these elements combine to reconstruct the self-image that an individual intends to project externally through the instrument of the Web. The biography represents the link between the two persons, the physical one and the digital one, according to two different modalities: in

becomes fluctuating and uncertain. It is a status characterised by a highly blurred distinction between real and virtual, as the distinction between man, machine and nature fades away. The greater availability of information brings with it the problem of guaranteeing the right to privacy and the transition from a binary concept of propriety and relations to an approach based on networks and processes. See Floridi 2015.

[17] Sullivan 2011, 5-10.

[18] Castells 2002, 22.

[19] Rodotà 2012, 273-276.

the case of a *natural person* it consists in the capacity to recognise oneself and have awareness of one's life plan; in the case of the *digital person*, by contrast, it consists in a sequence of fragments of one's own image. As a *disincarnate* projection of a physical body, the *digital person* acquires the rights and adopts the values held by the natural person in the real world.

However, it should be borne in mind that one's identity, both in the real world and in the digital world, is not static; rather, it is dynamic and changes over time. The *digital person* is intimately tied to the information making up that person: every addition or removal of information may have a significant impact on the digital ontological structure and, consequently, on the externally projected image.

The image of the *digital person* as a whole is known only to its owner, i.e. the individual who has moulded it with their own will[20]; the knowledge others have of it is limited, by contrast, to the data they come into contact with, that is, the *trail* of digital fragments left in the Web.

In this sense the *digital person* is a polymorphic entity that varies based on context and the nature of the data.

Therefore, *digital identity* as a concept differs from *digital person*: the former denotes a process of validation of a user connected to the Internet, who accesses information services (social platforms, electronic payments, etc.), where there may be multiple self-representations depending on the number of different profiles that can be created; the latter, by contrast, indicates the representation of the virtual image that can be obtained from data, subsequently transformed into information, which individuals enter online and which guarantees an *infinite virtualisation* of their social practices.

Digital identity does not seem to be linked to anything that people refer to as identity. Following thought experiment should explain what I mean.

If we were to look at 10 newly created Facebook profiles with no personal information, they all look the same to us. However, looking at the code that defines these profiles for Facebook's ICT infrastructure, you will find that these accounts are unique and different from each other by their exclusive "under the hood" identifiers. So now, let's get to the interesting part, say we make these 10 accounts have the same name, and fill them with the same social posts of real pictures. Let's also imagine they have the same family pictures. Now, what do you think it happens? From a human observer point of view, we would still find no difference between the accounts. However, the computer still does, making a distinct difference between what was posted by all 10 accounts, no matter the order.

[20] Ivi, 318.

What has really happened here? To put it simple, we have 10 different entities that interact with the Facebook platform, but for any of us, we would probably see only one, namely the same person. Here is the key point to discern and to help explain what this means: a single digital persona and 10 different digital identities have emerged as a result of the thought experiment. The digital persona article defines that a digital persona is "a part of the individual identity that has been extended into the online sphere to which corresponds a digital unconscious structuring a digitally divided self". My suggestion is to look it also in this way - digital persona is a collection of information that the cognitive and sensory mechanics of a human being parses into an individual actor, a character. This differentiation of digital identity and digital persona is crucial in creating better future ICT systems. Digital identity is something that is in the virtual dimension and does not directly interact with us, people, but interacts only with machines. Digital persona on the other hand, is what people use, to make sense of interactions in virtual space.

The difficulty of controlling and managing personal information once it is published online represents the most critical aspect of the *digital person* and their life on the Internet, especially given the number of connections of every individual linked to the network, as well as their potential vastity.

This has led to a veritable genetic mutation of data processing methods and how data is conceived: it has gone from being a fundamental component for the construction of an individual's *digital personality* with an immaterial value of exchange, to being part of an immense computing network, namely the Internet.

3. Personal data protection and the case of children in the GDPR

In the opinion of Antonello Soro, president of the Italian Data Protection Authority, upon the full implementation of Regulation (EU) 2016/679, the GDPR will represent the regulatory framework for addressing what will be one of the most important challenges of the coming decades: that of effectively safeguarding the fundamental right to the protection of personal data, which increasingly represents a crucial guarantee of freedom in the digital society and stands in a constant dialectic with a constantly evolving reality, being subject to the incessant developments of new technologies.

In line with the prevailing view of legal scholars[21], the European legislator no longer defines privacy in negative terms simply as the "right to be let

[21] Rodotà 1997; Frosini 2015, 101-115; Pagallo, 2014, 221-266; Pizzetti, 2016; Bilotta 1999.

alone", but rather as the right to have some form of control over one's personal data. The evolution of case law also come to reflect this new positive approach to the protection of privacy: the possibility of exercising a right of control over data concerning one's own person, data that has escaped from the negative and inalienable realm of privacy and become the input of a computer program.

Data privacy and data protection are closely interconnected, so much so that lawmakers, the courts and users themselves often consider the two categories as synonymous. However, making a distinction between data privacy and data protection is fundamental in order to understand the complementarity between the two categories. The privacy concerns arise where information tied to personal identification is collected, stored or used.

In short, data protection means safeguarding against unauthorised access or intrusions. Data privacy, on the other hand, regards authorised access to personal data in reference to the subject they belong to and the recognition of that access from a legal standpoint. Another way to understand this distinction might be to consider the protection and authorised processing of data as a technical problem and data privacy as a genuinely legal issue tied to a fundamental right, namely the right to protection of the inviolability of the human person and, more precisely, personal dignity.

Unlike the protection of privacy, reductively interpreted as the right to be let alone, the expression "data protection"—the traditional domain of security professionals—refers to the protection of data against unauthorised access.

In this case, concerns arise when personal information is collected, stored or used and the individual concerned has no control over these activities: the personal data can be shared with a third party "authorised" by the data controller (i.e. a data processor acting on behalf of the latter) and this could be perfectly sufficient to satisfy data protection requirements (for example information security), but might be unacceptable according to data privacy criteria, since the processors (third parties) might not have been "authorised" by the data subject, who may indeed be opposed to the processing.

In short, the GDPR joins together the principles of data protection and data privacy and establishes that people should have control over the processing and use of their data, while simultaneously assuring that the firms (which process the personal data) are liable for their actions.

When comparing data privacy with data protection, it is important to understand that the confidentiality of data cannot be guaranteed unless it is fully protected by digital technology. This is exactly what the drafters of the GDPR were unable or unwilling to take into account, given that Article 1 establishes that the regulation is designed to protect the fundamental rights and freedoms of natural persons, and in particular their right to the protection of personal data (that is, what takes place after the individual has waived their right to privacy).

The European legislator indirectly admits that online privacy is an illusion: data protection does not rule out the possibility that access thereto can be "contracted out" by the data controller to third parties operating in the digital market.

The current form and scope of the data protection approach is unlikely to adequately address a range of forms of attacks on personal information such as public disclosure of private facts by the media, surveillance and intrusion. Since data protection legislation only applies to automated or archival-based processing, it cannot cover most of the instant threats posed by paparazzi, snoopers, or hackers. Furthermore, since the media are an essential feature of a democratic society, their (misconduct) is subject to the jurisdiction of the ordinary courts and should not fall within the competence of data protection supervisors[22].

On the basis of this logic, the GDPR assigns a pre-eminent role to parental consent with the aim of protecting the personal data of children younger than sixteen online.

Globally, it is estimated that one out of every three Internet users is less than 18 years old[23]. Children not only enjoy the opportunity to play games, create, learn and express themselves, experiment with relationships and identities, but also, at the same time, they disseminate increasing amounts of personal data. Cloud Computing and growing *datafication*[24] have brought about an increase in the risks surrounding online privacy, e.g. risks of commercial exploitation and improper use of personal data, profiling, identity theft, damage to reputation and discrimination. For example, as a consequence of dataveillance via mobile (IoT) and wearable devices, social media platforms and educational software, children are considered like algorithmic assemblages, with the risk that their complexity, potentialities and opportunities may be profiled[25]. Moreover, due to their particular online behaviours[26], young teenagers appear to be more vulnerable than adults; indeed, evidence in the field of developmental psychology shows that adolescents are likely to be more active and inclined to take risks online.[27] They might not be able to correctly evaluate dangerous situations, not being fully aware of the consequences which, in the long term, may result from

[22] Wacks 2000.

[23] Livingstone, Carr and Byrne, 2015.

[24] Mayer-Shönberger and Cukier, 2013.

[25] Lupton and Williamson 2017, 780-787.

[26] Bessant 2008, 347-358.

[27] Hope 2007, p. 87.

their virtual actions.[28] These specific characteristics tied to the physiological development of children could be easily exploited by online marketing operators that collect personal data and use techniques such as real-time offers, geo-targeting (above all when the user is located close to a place of purchase) and ads tailored to individual profiles and behavioural models.[29]

Given these online risks, the GDPR acknowledges that children are in need of greater protection than adults: indeed, according to recital 38 of the regulation, they may be less aware of the risks, consequences and safeguards in place and their rights in respect of the processing of personal data, especially online. In order to guarantee special protection, the GDPR introduced broad changes in relation to the processing of children's personal data online; these include measures to ensure that the information intended for individuals falling within the specified age range is appropriate, a strengthening of the right to erasure and enhanced protection against marketing and profiling. The main provision regarding children is set forth in Article 8 "Conditions applicable to child's consent in relation to information society services", according to which the processing of data is lawful where the child concerned is at least 16 years old (unless a national minimum age of between 13 and 16 years is applied)[30]. If the child has not yet reached that age, the processing of data will still be considered lawful, but only where "consent is given or authorised by the holder of parental responsibility". It follows that children under sixteen years of age cannot join any social network or register with any content sharing platform or website that collects their personal data. Under Article 8(2) the data controller must verify that consent has been duly given or authorised by the holder of parental responsibility.

According to the provisions of the GDPR, the enforcement of general requirements for lawfully obtaining consent is undoubtedly even more complex when it comes to children's consent online. For example, in cases where children might give their consent without their parents' involvement, it would be much more difficult to consider their consent to be "freely" given, as their vulnerability would very often be exploited for commercial reasons and their choices would subject to manipulation. It is not simple to ensure conditions in which we could talk about children's "informed consent", since they do not possess the same ability as adults to analyse the possible

[28] Giedd 2008, 335.

[29] Montgomery 2015, 771.

[30] In Italy the minimum age for giving consent to information society services has been set at 14 years. The orientation of our legal system changed with Legislative Decree no. 101/2018, which entered into force on 19 September 2018, given that the draft decree approved on 10 August 2018 had confirmed the age of 16 years as the minimum for accessing web services, in accordance with the GDPR.

consequences. Although it is common practice to use privacy policies, many of which formally address the legal aspects related to mandatory information, it is doubtful that they achieve their purpose[31].

Given the complexity of profiling and big data analysis techniques, the majority of children, even when plenty of information is available to them, would be incapable of understanding what impact expressing their consent would have on their privacy. Many privacy policies are complex, difficult to implement and rely on unintelligible language that is even beyond the comprehension of an average adult.

Moreover, such difficulties are further compounded by the fact that the GDPR requires the data controllers to obtain parental consent before processing the personal data of children, but there is no prior obligation for them to verify the child's age. That should not come at all as a surprise: first of all, this issue still raises many sensitive and unresolved questions regarding anonymity, freedom of speech and expression and privacy of both children and adults online. Although age verification is the legislative solution adopted for gambling or the online sale of products subject to age limits at a European level, this is not the case for privacy-related risks and data protection, where a detailed, reliable database of evidence is still lacking. Verifying people's age in order to distinguish between minors and adults who are 18 years of age or older is what service providers do to control access to damaging content, such as offensive or sexually explicit online content.

Practically speaking, content that is unsuitable for children is hidden by a "wall" that can be circumvented with payment methods restricted to adults (e.g. credit cards); however, age could also be established using an independent and reliable source, such as a database of eligible voters. Yet none of these methods is appropriate for the purpose of implementing the GDPR, since the age thresholds (13-16 years) are different and do not coincide with the age of majority (18 years). This means that there is a limited number of reliable databases with information about children's age, since the majority of databases (social security numbers, passport numbers) only allow us to determine whether an individual is an adult: there is no possibility of obtaining granularity as far as age is concerned. A cross-check in public databases may provide reliable information, but is technically complex to implement; moreover, the delicate nature of the data to be handled poses enormous privacy concerns.

[31] Van Eecke and Truyens, 2010, 542.

Finally, consent cannot be considered freely given when any refusal to give such consent results in a child being socially excluded and important online services do not offer real alternatives[32].

In conclusion, and for all the above reasons, the protection of children's online privacy has been reduced to a marginal problem.

4. Web architectures and social communication

Technology has always had inherent normative consequences. However, with the emergence of digital technology, it becomes highly apparent. Digital development has affected law in a gradual manner. The first step is related to information technology, more specifically to the collection and storing of data of various kinds. With the emergence of the internet of things (IoT) this grew tremendously which made regulation and restrictions important. The second step in the digital development is when the substratum of law goes from real space to virtual space, e.g. when physical property more and more turns into intellectual property, when digital money is introduced and when contracting is more and more about service instead of goods. The third step begins when the technology itself starts to become normative. Code is law as Lawrence Lessig explained it more than two decades ago. With the introduction of algorithms and AI, normativity is no longer just a matter of how technology is programmed and used, but how it becomes an inherent part of the technology[33].

The *informational coding* of law has led to an irreversible crisis of state sovereignty: due to its rigidity, state law has revealed to be incapable of governing the new realms of human action; destatalization and delocalization have produced a flexible law, which adapts to the network-based model of the digital world.

As a proponent of the 'code-based approach'[34] developed by Lawrence Lessig[35] and Joel Reidenberg,[36] I believe that the architecture of cyberspace is not established by default, but rather as a function of its code. The code is ever changing: its particular evolution may be determined by the government, or by multinational corporations. The architecture of cyberspace is not neutral. Where code-based architectures have an impact on legal constraints, they also end up supplanting the fundamental values and principles of law. In

[32] Furlong and Keri 2001, 451.

[33] Hydén 2020.

[34] Regarding the code-based approach, see Weber 2015.

[35] In computer science, "code" typically refers to the text of a computer program (the source code). In law, "code" can refer to the texts that constitute statutory law. See Lessig 1999.

[36] Reidenberg 2005.

the case of intellectual property, for example, the code appears to be more inclusive than the law: the latter favours an architectural implementation of the code which benefits holders of large percentages of intellectual property, thus exempting telecommunications multinationals from responsibility for providing universal service and sharing networks. In the field of copyrights, digital architecture—i.e. the way in which technologies determine *ex ante* the boundaries of user behaviour—has progressively narrowed the margins of freedom (fair use) with respect to individual choice. The architecture, built upon a binary numerical system[37], has placed strong constraints on individuals, highly limiting their ability to act: digital property, for example, is a form of communication that becomes a mimetic property of the architecture (every use of a creative work automatically generates a copy) and now imposes controls and rules influencing the law and the market[38].

Most notably, Lawrence Lessig developed the idea that code is law, that law and behavior-modifying regulation exist in digital environments, but that they manifest in different ways, most effectively through architectural and material means[39].

In Lessig's opinion, from now on controls on the access to content will not be ratified by courts, but will rather be implemented by programmers via the code. Unlike the controls introduced by law, those imposed by technology are not subject to judicial verification[40]. Furthermore, whereas a legislative rule (expectation of action) can be scrutinised and challenged, the same cannot be said for technological rules (expectation of communication)[41].

Put more simply, the Internet is governed by technical rules of the type: "if you want R, you must necessarily do S". If an act does not fulfil a technical obligation, it will not achieve the intended purpose. Normative provisions within the Internet are technical rules designed so that the chain of consequentiality precludes disobedience: they are communicative acts that produce effects at the moment and by virtue of the fact that they

[37] In Luhmann's view, binary codes are duplication rules whereby information, in the process of communication, is evaluated and compared with a precisely corresponding counter-value, no third option being possible; see Luhmann (1989, 107). In addition, he holds that the selectivity of a communication is attributed to itself: it constitutes its own meaning, and individuals react by making their own behavioural choices not on the basis of pre-established solutions, but rather on the basis of information about selective performances of others; see Luhmann and Febbrajo (1995, 33).

[38] For example, the system outlined by Digital Rights Management (DRM) imposes contractual clauses and conditions restricting the use of digital property. Through a pervasive control that invades the consumer's privacy, the owner of the content—more so than the legislator—determines the balance between proprietary interests and the enjoyment of content.

[39] Bietti 2021.

[40] Lessig 2005, 124 ff.

[41] Caso 2007.

are articulated. A technical rule does not prescribe adaptation, but rather implements it.

Society, by contrast, is generally governed by prescriptive conditional rules of the type: "if it is X, then it must be Y". Certain behaviours are to be adopted, but they are defined in deontic conditional terms, and thus do not take place at the moment the rule (which may well be broken) is laid down. A deontic norm prescribes adaptation, but does not implement it, nor is it concerned with whether it is implemented.

Accordingly, in Luhmann's opinion, deontic or prescriptive norms, unlike technical ones, do not impose (do not presuppose) conforming conducts, but rather protect against those who fail to adhere to them. Where this protection is difficult, law tends to become socially deflated[42]. This is exactly what occurs in the digital environment.

Ultimately, "Code is law" is a form of regulation whereby technology is used to enforce existing rules. With the advent of Blockchain and Machine Learning, we are witnessing a new trend, whereby technology is progressively taking the upper-hand over these rules. Yet, as opposed to traditional legal rules, which merely stipulates what people shall or shall not do, technical rules determine what people can or cannot do in the first place. This eliminates the need for any third-party enforcement authority to intervene after the fact, in order to punish those who infringed the law. Moreover, as laws are incorporated into a code-based system whose rules dynamically evolve as new information is fed into the system, it might become difficult for people to not only understand, but also question the legitimacy of the rules that are affecting their lives on a daily basis.[43]

In order to balance the limits and possibilities of behaviour in cyberspace, it is thus necessary for there to be a continual interaction between state or supranational regulation and the code architecture (or *Lex informatica*).

An implicit barter takes place between the provider of an IT service and users: users who want to use the provider's platform and create their own virtual space must "consensually" provide their data to the platform owner.

This implies a veritable genetic mutation of data processing and how data is conceived, since it becomes part of an immense computing network, namely the Internet: data is transformed from a fundamental component for the construction of an individual's *digital personality* into an intangible object of exchange. All digital information is reproducible at marginal costs: the user's acceptance of all the provisions constitutes a pretense of agency, while the corporations that hold intellectual property rights and defend

[42] Luhmann 2013.

[43] Hassan and De Filippi 2017.

them against fair use transform digital information into a scarce good to be profited from.

5. Virtual bodies: between habeas corpus and habeas data.

Samuel D. Warren and Louis D. Brandeis were the first jurists to define and systematise the right to privacy[44]. In their essay they define it as a negative right, a *right to be let alone*, because it is designed to protect individuals who demand that information regarding their intimate, ideological, family and sexual spheres be kept confidential.

A right thus defined implies that any public or private actor will be prohibited from keeping an individual under surveillance or interfering in their private sphere, except in the specific cases provided for by law. The right to privacy has become extremely dynamic and changeable as a result of technological evolution; new aspects of life are affected and thus new forms of protection need to be introduced.

Personal data needs to be defended not only against the violation of secrecy and undue publication by third parties[45], but also against the risk of being manipulated once it has been entered into largely uncontrollable communication and dissemination systems.

Today, because of this evolution and in response to the demands progressively and incessantly expressed by *digital sociality,* the original core of the right to privacy has been expanded to embrace new circumstances. These include the right to control the use, by third parties of information regarding a person[46] and the right not to have one's information altered. The recognition of the right to defend one's life choices[47] has made privacy a fundamental aspect and a precondition for the full enjoyment of the right to self-determination, as well as the right to build one's own identity and adopt all measures to prevent each person from being simplified, objectified and judged out of context[48].

Privacy thus has a dual significance. On the one hand, the right to privacy protects personal information against control by others; on the other hand, it is geared towards protecting the self-determination of one's life plan, a constituent element of the private sphere[49] of each individual. In short, the

[44] Warren and Brandeis 1890.

[45] Samuelson 1999.

[46] Westin 1970.

[47] Friedman 1990, 184.

[48] Rosen 2000, 20.

[49] Rodotà 1995, 122.

expansion of the meanings and protections associated with privacy is aimed at protecting personal integrity and dignity.

Personal data protection cannot be limited to mass media outlets such as newspapers and television (already subject to *ad hoc* rules); it must be extended to the Internet, given its ubiquitous presence in every sector of society.

Those who control the market of information production and distribution establish which commodities will be taken into consideration and, therefore, which information will be officially accessible in the "personal data market".

IT corporations come into possession of data regarding various aspects of our lives: ideological orientation, religious orientation, sexual preferences, financial transactions, consumption habits, biometric data (fingerprints, retinal scanning) and genetic data[50].

If we think about it, these are data that, taken together, reflect the most important interests and experiences in people's lives, to the extent of baring their ontological essence[51].

In such a context, the safeguards that need to be put in place grow considerably: in addition to providing protection against the dissemination of information regarding an individual's public image, it is necessary to ensure that third parties refrain from storing and manipulating data which, in most cases, consists of digital traces that are impossible to erase; even where personal data have been anonymised, the application of the reverse process, re-identification, always remains a possibility.

As a large part of computational processes are hidden to users, the contemporary meaning of privacy refers to the protection of data belonging to individuals and related to their personality, irrespective of the place where it is expressed.

For example, with cloud computing technology users can upload their computer activity to a virtual environment accessible via a browser, so they are able to exploit the storage space offered by the provider only by connecting to the Internet. The data is transferred to a storage medium (Dropbox, Google Drive, OneDrive, etc.) that is beyond the control of the file's creator and owner. This operation takes place legally: it is the users themselves who accept and confirm the terms and conditions of cloud computing contracts, but the service provider does not offer sufficient information about the use that will be made of the acquired data or the processing it will undergo.

[50] Wacks 2010, 10-12.

[51] Ivi, 21-22.

The *digital person* is the result of data produced by a natural person: an electronic device, body-information, body-password[52]. In short, it is a receptacle of collected, processed data and information forming a person's *digital biography.*

The *person,* though transformed from both a genetic (*cyborg*) and cybernetic (*inforg*) point of view, maintains intact the right to dignity and to choose the information that may be known by society via the Web.

Just as physical integrity is protected against public power by *habeas corpus*, in the digital context the *digital person*'s body is protected by *habeas data*[53]*;* the latter provides for the intangibility of the public image produced by the data entered online (*digital right to privacy*) and protection against undue manipulation of one's data by third parties (*right to data protection*).

Habeas data represents the right of *digital persons* not to have their virtual bodies manipulated by external agents, either by their own consent (otherwise the fundamental nature of the right would be reduced to a simple subjective right *ad rem*) or by a competent authority where not authorised. This new form of sovereignty over digital personal data underpins the protection of the sphere of individual privacy, and the new conception of privacy itself.

The principle of *habeas data* obviously does not imply enabling personal data to be shared; rather it aims to protect the overall image an individual identifies with and wishes to project outwardly, without the interference of another actor that manipulates or alters it. However, to prevent a deviation of *habeas data* from a contractual standpoint, it is necessary not to separate it from the principle of *habeas corpus*: each of these two principles responds to the need to defend the individual from abuses of power on the part of the authorities and to protect the right of the *digital person* to dignity and self-determination, both online and in the real world. Our existence as separate individuals and our personal identity are founded on the fact that we are *bodies.* The network of computers has made the physical presence of participants redundant by omitting or simulating the immediacy of the body. The dark side of this cybernetic operation implies that it is the mind which governs our organic life. Yet can we ever be completely present when we live through a surrogate or virtual body that stands in our place?

The joint protection of *habeas corpus* and *habeas data* represents the latest frontier as regards the global protection of individuals: the human body is the point zero of the world; it is "like the City of the Sun. It has no place, but it is from it that all possible places, real or utopian, emerge and radiate"[54].

[52] Cristofari 2013.

[53] Rodotà 2014, 27-32.

[54] Foucault 2006, 43.

References

Augè, Marc. *Nonluoghi: introduzione ad un'antropologia della surmodernità.* Elèuthera, Milano 2009.

Bietti, Elettra. *A Genealogy of Digital Platform Regulation. SSRN 3859487* (2021).

Bilotta, Francesco, *L'emersione del diritto alla privacy.* In *Clemente A. (a cura di), Privacy, Cedam, Padova* 1999, pp. 21-61.

Cardon, Dominique. *Che cosa sognano gli algoritmi.* Edizioni Mondadori, Milano 2018.

Caso, Roberto. *L'immoralità delle regole tecnologiche: un commento a Burk e Gillespie.* In Ziccardi G. (a cura di), *Nuove tecnologie e diritti di libertà nelle teorie nordamericane, Mucchi, Modena* 2007.

Castells, Manuel. *La nascita della società in rete.* EGEA, Milano 2002.

Cristofari, Fabiuana. *Gli algoritmi dell'identità: il corpo umano*, in Amato S. - F. Cristofari - S. Raciti, *Biometria. I codici a barre del corpo*, Giappichelli, Torino 2013, pp. 43-45.

Facer, Keri, and Ruth Furlong. *Beyond the myth of the 'cyberkid': Young people at the margins of the information revolution.* In *Journal of youth studies* 4, no. 4 (2001), pp. 451-469.

Floridi, Luciano. *La rivoluzione dell'informazione.* Codice, Torino 2012.

Floridi, Luciano. *The onlife manifesto: Being human in a hyperconnected era.* Springer Nature, London 2015.

Foucault, Michel. *Sorvegliare e Punire. La Nascita della Prigione*, (tr. it. a cura di A. Talchetti), Einaudi, Torino 2014.

Foucault, Michel. *Utopie. Eterotopie.* Cronopio, Napoli 2006.

Friedman, Lawrence Meir. *The Republic of Choice: Law, Authority, and Culture.* Harvard University Press, Cambridge 1990.

Frosini, Tommaso Edoardo. *Liberté Egalité Internet*, Editoriale Scientifica, Napoli 2015.

Håka Hydén, *Sociology of Law and artificial Intelligence.* in Jiri Priban (ed), *Research Handbook on the Sociology of Law*, Elgar Publishing, Cheltenam/Northampton 2020, pp. 370-384.

Lessig, Lawrence. *Cultura libera. Un equilibrio fra anarchia e controllo, contro l'estremismo della proprietà intellettuale.* Apogeo Editore, Adria 2005.

Lessig, Lawrence. *Code and Other Laws of Cyberspace.* New York, 1999.

Livingstone, Sonia, John Carr, and Jasmina Byrne. *One in Three: Internet Governance and Children's Rights. In Global Commission on Internet Governance Paper Series,* No. 22 (2015), CIGI Press, Ontario, Canada.

Luhmann, Niklas, and Alberto Febbrajo. *Procedimenti giuridici e legittimazione sociale.* Giuffrè, Milano 1995.

Luhmann, Niklas. *Comunicazione ecologica.* Franco Angeli, Milano, 1989.

Luhmann, Niklas. *Esistono ancora norme indispensabili?* Armando Editore, Roma 2013.

Hassan, Samer, and Primavera De Filippi. *The expansion of algorithmic governance: from code is law to law is code.* In *Field Actions Science Reports. The journal of field actions. S*pecial Issue 17 (2017), pp. 88-90.

Lupton, Deborah, and Ben Williamson. *The datafied child: The dataveillance of children and implications for their rights.* In *New Media & Society* 19, no. 5 (2017), pp. 780-794.

Bessant, Judith. *Hard wired for risk: Neurological science,'the adolescent brain'and developmental theory.* In *Journal of Youth Studies* 11, no. 3 (2008), pp. 347-360.

Hope, Andrew. *Risk taking, boundary performance and intentional school internet "misuse".* In *Discourse: studies in the cultural politics of education* 28, no. 1 (2007), pp. 87-99.

Giedd, Jay N. *The teen brain: insights from neuroimaging.* In *Journal of adolescent health* 42, no. 4 (2008), pp. 335-343.

Lyon, David. *La società sorvegliata. Tecnologie di controllo della vita quotidiana.* Feltrinelli Editore, Milano 2002.

Mayer-Schönberger, Viktor, and Kenneth Cukier. *Big data: una rivoluzione che trasformerà il nostro modo di vivere e già minaccia la nostra libertà.* Garzanti, Milano 2013.

Montgomery, Kathryn C. *Youth and surveillance in the Facebook era: Policy interventions and social implications.* In *Telecommunications Policy* 39, no. 9 (2015), pp. 771-786.

Pagallo, Ugo. *Il diritto nell'età dell'informazione: il riposizionamento tecnologico degli ordinamenti giuridici tra complessità sociale, lotta per il potere e tutela dei diritti,* Giappichelli, Torino 2014.

Pizzetti, Franco. *Privacy e il diritto europeo alla protezione dei dati personali: Dalla Direttiva 95/46 al nuovo Regolamente europeo.* G Giappichelli, Torino 2016.

Popper, Karl R. *I tre mondi: corpi, opinioni e oggetti del pensiero.* Il Mulino, Bologna 2012.

Reidenberg, Joel R. *Technology and Internet jurisdiction.* In *University of Pennsylvania Law Review* 153, no. 6 (2005), pp. 1951-1974.

Rodotà, Stefano. *Il diritto di avere diritti.* Laterza, Roma-Bari 2012.

Rodotà, Stefano. *Il mondo nella rete: quali i diritti, quali i vincoli.* Laterza, Roma-Bari 2014.

Rodotà, Stefano. *Tecnopolitica. La democrazia e le nuove tecnologie della comunicazione.* Laterza, Roma-Bari 1997.

Rodotà, *Tecnologie e diritti*, Il Mulino, Bologna 1995.

Rosen, Jeffrey. *The unwanted gaze: The destruction of privacy in America.* Random House, New York 2000.

Rushkoff, Douglas. *Programma o sarai programmato. Dieci istruzioni per sopravvivere all'era digitale.* Postmediabooks, Milano 2012.

Samuelson, Pamela. *A New Kind of Privacy-Regulating Uses of Personal Data in the Global Information Economy.* In *California Law Review*, 87 (1999), pp. 751-766.

Sullivan, Clare. *Digital Identity: an emergent legal concept.* University of Adelaide Press, South Australia 2011.

Van Eecke, Patrick, and Maarten Truyens. *Privacy and Social Networks.* In *Computer Law & Security Review* 26, no. 5 (2010), pp. 535-46.

Wacks, Raymond. *What Does Data Protection Have To Do With Privacy?.* In *Privacy Policy and Law Reporters* 143 (2000), s.p.

Wacks, Raymond. *Privacy: A very short introduction.* OUP, Oxford 2010.

Warren, Samuel D., and Louis D. Brandeis. *The Right to Privacy.* In *Harvard Law Review* 4, no. 5 (1890), pp. 193–220.

Weber, Rolf H. *Realizing a New Global Cyberspace Framework. Normative Foundations and Guiding Principles*, Berlin, 2015.

Westin, Alan. *Privacy and Freedom*, Atheneum, New York 1970.

Zarsky, Tal Z. *Governmental data mining and its alternatives.* In *Pennsylvania State Law Review* 116 (2011), pp. 285 ff.