

# Digital Integrity: A Foundation for Digital Rights and the New Manifestation of Human Dignity

**Lusine Vardanyan**  
**Václav Stehlík**  
**Hovsep Kocharyan**

Palacký University Olomouc  
Křížkovského 511/8  
Olomouc 77147, the Czech Republic  
Email: lucyrossetti77@gmail.com  
Email: vaclav.stehlik@upol.cz  
Email: hovsep.kocharyan01@upol.cz

**Abstract:** The article is devoted to the research of the problematic aspects and modern challenges of data protection in the digital age from the perspective of the digital integrity of the person. We believe that personal data cannot be effectively protected as components of digital integrity of the person in the context of regulation of a separate right to personal data protection, which, in its turn, acts more as a tool of market regulation rather than a classical fundamental right. We argue that the consideration of digital integrity as a new foundation for digital rights and as a new manifestation of the restrictive concept of human dignity may help increase the level of effective protection of the person in the digital sphere as well as properly cover the existing gaps in the protection of the digital rights of the person.

**Keywords:** *commodification, digital integrity, dignity, internet, personal data*

## 1. Introduction

In the context of digitalization of our lives, personal data has already been recognized as one of the key economic assets. “The fourth industrial revolution, in which we transit, is preceded by a digital economy based fundamentally on information. And although estimates have been made on whether the data moving in the digital economy flow are from sensors or machines or come from each of us, one thing is certain, all information has a monetary value” (Becerril, 2018). At the same time, the issue of the development of an effective data protection strategy as an important part of the process of forming the EU single digital market comes to the fore (Ježová, 2020). In this context, the leading role of the EU in data economy is stipulated with tackling issues ranging from connectivity to the processing and storage of data, improving its governance structures for handling data and increasing its pools of quality data available for use and reuse (Hamulák *et al.*, 2021). However, creating such a single digital market increases threats to privacy and the commodification of personal attributes. As a result, the EU is forced not only to develop an appropriate legal framework for creating a digital data market, but, at the same time, minimize such threats and challenges.

Besides, the possibilities of creating a digital profile of a person from his/her “digital parts” make the problems of the comprehensive protection of his/her personal data more acute. In this regard, the EU legislators pinned their hopes on the General Data Protection Regulation (hereinafter the GDPR), which entered into force on May 25, 2018. However, despite the GDPR’s attempt to provide comprehensive data protection, there are still many unresolved issues in this area of law (Kocharyan *et al.*, 2021). Among them is the problem of fragmentation of the personal data protection in the conditions when “non-processed” personal data remains outside the scope of the GDPR. In addition, the GDPR does not contain legal mechanisms to protect personal data from hacker attacks, against the use of personal data in the field of political targeting (such as in the case of Cambridge Analytica), or data collection for reasons of national security.

Moreover, another serious problem for the GDPR is the issue of human privacy protection in the conditions of the Covid-19 pandemic: against the background of the pandemic, geolocation tracking, face recognition system deployment, software pre-installation obligations and phone tracking are taking place. The Covid-19 pandemic has opened new horizons for mass

surveillance, making it easier, and has expanded the possibilities of collection of information on a person (Vardanyan & Stehlík, 2020).

All these above-mentioned types of data collection are usually excluded from the scope of the GDPR, despite the fact that this legal instrument, as indicated in the case-law of the CJEU, is considered as the implementation of the fundamental right to personal data protection.

The objective of this article is to show the existing gaps in data protection in the EU and suggest a reasoned way to increase the effectiveness of data protection in the EU by considering the right to digital integrity as a new foundation for digital rights and a new manifestation of the restrictive concept of human dignity.

To achieve the research objective and solve the complex issues of the paper, we used several approaches. In particular, as a starting point (working with a set of relevant data/documents), we employed the analytical approach (the desktop research) in order to identify, systematize and mutually compare the provisions of the GDPR, key case-law of the European supranational courts, its impact and interpretations. In addition, we also used a deductive approach when testing our hypotheses against the assembled data; the inductive method when formulating the models of interpretation; the comparative method when comparing the provisions of appropriate legislative acts and judicial cases; synthesis when working on the conclusions; and prediction in evaluation and extrapolation of the future developments.

This research tries to find answers to the following questions:

- Does the right to personal data protection itself effectively protect personal data as a component of personal identity in the digital world in the EU?
- Will digital integrity as a new foundation for digital rights and as a new manifestation of the restrictive concept of human dignity help increase the level of effective protection of the person in the digital world in the EU?

## 2. Literature review: the current situation

There are a number of researches devoted to analyzing the essence, nature and content of the right to personal integrity and the issues of its legal protection in Europe (Hill, 2016; Kerikmäe, Hamulák & Chochia, 2016; Herring & Wall, 2017; Ruggiu, 2018; Usera, 2017; Patella-Rey, 2018; Joamets & Chochia, 2020; 2021). Most of the researchers examine the right to personal integrity within the framework of the right to private life (privacy) or the right to data protection (de Andrade, 2011; Kokott & Sobotta, 2013; Brkan & Psychogiopoulou, 2017). Of particular interest is the research conducted by Cecilia Magnusson Schoberg (2018), who pointed out that information security is crucial for the protection of personal integrity.

The potential change in the accepted ontology of the body ('body as data') and entry into force of the GDPR raise the problem of a broad interpretation of the concepts of 'information' and 'data'. The possibility of including human biomaterials in the material scope of the GDPR is a topic for a set of research (Bygrave, 2015; Purtova, 2018; Urgessa, 2016); however, the feasibility of such a scenario is doubtful. In particular, Article 1(2) of the GDPR specifically emphasizes that the Regulation "protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data". It is possible to see that the GDPR provides an autonomous mode of personal data protection and weakens the protection of the person while the processing of data is "digitizing" him/her. At the same time, the GDPR is not able to protect the person's personal data against mass surveillance, hacker attacks and/or data collection for national security reasons, which are the fundamental risks for the person and his/her "wholeness" in the digital world. In this framework, the question of finding other fundamental guarantees for the protection of the person in the digital sphere becomes critical.

Taking into account the specified threats and challenges, very few researchers suggest recognizing a new fundamental right—the right to digital integrity as an extension of the right to personal integrity (Roussel, 2020; Rochel, 2020; Mahon, 2020; Kuhn, 2020). However, the studies do not consider the problematic aspects of the correlation of the right to digital integrity with the right to physical integrity of the person and the right to data protection in the context of "body as information" ontology. Meanwhile, the clarification of the strict limits and content of these rights is important not only in philosophical and theoretical, but also in normative and practical terms because it will be able to play a significant role in the further development of the EU law.

The relevance of the research derives from the fact that the rapid development of information technologies has led to the need to address issues related to improving security guarantees in the digital sphere. This research will help assess the possibility of the right to digital integrity as an alternative legal framework and foundation for the protection of digital rights.

### 3. The right to personal data protection: a protective tool for compromises but not for individual interests

Article 7 of the CFR stipulates that “[e]veryone has the right to respect for his or her private and family life, home and communications”, while Article 8(1) of the CFR provides that “[e]veryone has the right to the protection of personal data concerning him or her”. Unlike the CFR, the European Convention on Human Rights (hereinafter the ECHR), in its turn, does not contain any special right to personal data protection, and the issues related to the violation of personal data are usually considered in the context of the right to private life (privacy) (Art. 8(1) of the ECHR). As Kokott and Sobotta point out:

privacy and the protection of personal data are closely linked in the jurisprudence of the European Court of Human Rights and the Court of Justice of the European Union, but they should not be considered to be identical. [...] [T]here are considerable overlaps in the scope of both rights, but also some areas where their personal and substantive scope diverge. (Kokott & Sobotta, 2013)

However, the issue of the correlation of these two fundamental rights still remains “vague” and problematic in the EU law: even if the CFR recognizes the right to data protection as a separate fundamental right, in the framework of considering of the scope of application of this right, we intuitively “slip” into the sphere of privacy. And maybe not just intuitively. Even if Article 16 (1) of the TFEU states that “[e]veryone has the right to the protection of personal data concerning them” and the CFR in its Article 8(1) indicates the emergence of an independent right to personal data protection, separate to that of privacy, Directive 2002/58/EC or Directive 2006/24/EC continued to maintain this connection. It is also noticeable in the text of Directive 95/46/EC (hereinafter DPD), where the word ‘privacy’ is repeated many times (Kocharyan *et al.*, 2021).

As we can see, the EU law attaches special importance to the right to personal data protection and elevates it to the rank of fundamental rights. It finds its consolidation as an independent right not only in EU primary law (in Art. 16 (1) of the TFEU and Art. 8 (1) of CFR), but also in the case-law of the CJEU (joined cases in *Rechnungshof v. Österreichischer Rundfunk and Others and Christa Neukomm and Joseph Lauerermann v. Österreichischer Rundfunk* [2003]; *Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD)*, *Mario Costeja González* [2014]; *František Ryneš v. Úřad pro ochranu osobních údajů* [2014]; *Maximillian Schrems v. Data Protection Commissioner* [2015]; joined cases *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources, and Others* [2014]), and such legal regulation is indisputable.

It should be noted that according to the case-law of the CJEU, fundamental rights are considered to be general principles, drawn from constitutional traditions common to Member States and from international agreements on human rights (*J. Nold, Kohlen- und Baustoffgroßhandlung v. Commission of the European Communities* [1975]). However, it is not possible to find such a general basis for the right to data protection in the constitutional traditions, since the constitutional traditions of the EU Member States put completely different values at the heart of the right to data protection. This means that the right to data protection as an independent fundamental right does not have a clear and definite legal basis as do other fundamental rights. We believe that it is more a result of the traditional approach of legal positivism: it is fundamental, since it is included in the CFR.

Moreover, the recognition of the right to personal data protection as a fundamental right in the CFR is somewhat doubtful, since it is strikingly different from other fundamental rights: it protects the compromise between the rights and interests of data subjects and data controllers, including the interests of enterprises and the state in data processing, while almost all fundamental rights protect individual interests (van der Sloot, 2017).

After all, along with the purpose of protecting individuals in relation to the processing of personal data, the goal of the GDPR is to assure the free movement (flow) of personal data (Art. 1 and Art. 51(1); recitals 6, 13, 53 and 123 of the GDPR). This goal is not secondary for this legal instrument: as one can see, some provisions of the GDPR, such as Article 1(3) of the GDPR, directly prevent Member States from restricting or prohibiting the free movement of personal data within the Union for reasons connected with the protection of natural persons with regard to the processing of personal

data (Art. 1(3) of the GDPR). As Andrea Monti and Raymond Wacks tend to believe:

The EU approach is based on a set of provisions requiring compliance with duties regarding data integrity, data availability, need to know and confidentiality. Of these four pillars, only the last is directly connected to the protection of personal information; the other three actually advance the precise opposite: allowing personal data to circulate (relatively) freely. (Monti & Wacks, 2019)

Indeed, these principles in their essence are aimed at ensuring the freedom of circulation of personal data, and therefore they cannot be turned into principles that provide the protection of human privacy. In this context the CJEU even declared that “according to settled case-law, the provisions of a directive must be interpreted in the light of the aims pursued by the directive and the system it establishes” (*Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy* [2008]), which was also repeated by the CJEU in the case *Sergejs Buivids v. Datuvalstsinspekcija* [2019]).

It is possible to notice that, in its case-law, the CJEU has prioritized the telos of protecting the rights of individuals over the free flow of data. The interpretation of these principles solely in the context of human rights protection still artificially distorts the essence of the GDPR and narrows the material scope and meaning.

The protection of individuals in the scope of the GDPR is not a goal but a means of creating a functional internal market and this compromise between the free flow of information and the protection of personal data is also one of the differences between the right to data protection and all other fundamental rights.

#### 4. The right to personal data protection: the right with the “market” basis?

The promotion of the free flow of information suggests that the right to personal data protection also affects the regulation of the EU data market. The GDPR regulation is “an essential step to strengthen individuals’ fundamental rights in the digital age and facilitate business by clarifying rules for companies and public bodies in the digital single market” (European Commission, n.d.). In addition, one of the pillars, which the Digital Single

Market Strategy of Europe (2015) is based on, is creating the right conditions for digital networks and services to flourish and the data protection falls under this pillar (A Digital Single Market Strategy of Europe, 2015). In its turn, the Digital Single Market Strategy specifies two legal instruments as the regulator of this sphere, one of which is the GDPR. Therefore, this right is an important instrument of data market regulation. Besides, the understanding of the GDPR as the instrument of implementation of this right means that the real sources of this right can be found namely in the market regulation and the free flow of information.

The very free flow of information, and the economy based on it, directly give rise to the problem of personal data commodification, even in the condition of the existence of the fundamental right to personal data protection. For example, the scandal around Cambridge Analytica has shown that it is an absolutely non-transparent market where personal data is a commodity. However, personal data is the basis of the economic model of the digital age and the GDPR provisions suggest that restricting exchange of personal data is an unacceptable option. At the same time, the adopted hybrid model of GDPR regulation, which, on the one hand, tries to protect human rights through data protection, and on the other hand, allows the EU Member States and companies to use personal information, uses property rights and remedies that are inherent in the protection of property relations. Commodification of personal data, which is not expressly established by EU law, is in this case imposed by itself. The European Commission's willingness to implicitly use property rights and remedies in this area demonstrates this direction of further development of the EU legislation. Besides, it also indicates that there is no objection to the fact that the identity elements of the person are commodified and become sources of profit.

The GDPR excludes data processing for statistical or research purposes from the scope of data protection if the data is provided anonymously. In other words, individuals do not have the right to data protection if their data is collected in an identifiable way but subsequently becomes anonymous. However, nowadays some researchers indicate that absolute and irreversible anonymity is no longer possible (Ohm, 2000, pp. 1701, 1742 et seq. and 1759; Schwartz & Solove, 2011, pp. 1814, 1877) and the data protection principles of the GDPR are not sufficient to prevent the commodification of personal data. All that the GDPR provides is that the data subjects are informed on how their right to privacy and other rights are being threatened and that they can more easily give their consent to this. The *de facto* functioning personal data market raises important ethical issues that cannot be resolved

at the GDPR level, since the GDPR does not lay down any specific rules on ethics. In particular, the Ethics Advisory group in the report *Towards a Digital Ethics* (2018) pointed out that the right to data protection does not seem sufficient to understand and address all the ethical problems caused by recent digital technological developments, and that “personal data protection regimes, like the GDPR, [...] appear inadequate to address the unprecedented challenges raised by the digital turn.”

Thus, we may conclude that the sources of this right are partly embedded in the regulation of the market and the promotion of the free flow of information, which means that this right is more an instrument of market regulation rather than a classical fundamental right.

## 5. What actually protects the right to personal data?

In order to understand what actually protects this right, it is necessary to understand what “personal data” is and how it is defined in the GDPR. Thus, the GDPR defines personal data as

*any information* relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. (Recital 4(1) of the GDPR)

As can be seen, the GDPR treats data and information as synonymous, while in the legal theory the disputes are mainly based on a conceptually clear distinction between the form of information and the information itself (Malgieri, 2016, p. 133; De Franceschi & Lehmann, 2015). At the same time, this distinction is not supported by the GDPR: on the contrary, by using synonyms ‘data’/‘information’, we tend to believe that the GDPR makes protection of both possible—the form of information and the information itself.

It is possible to assume that the characteristics of the data depend on the nature of the information: if the information contained in the data is personal, then the data is personal. This circumstance focuses our attention on the position that:

EU law defines personal data reversely: data is the source of information which, if personal, reversely implies that the original data is also personal. This definition leads into a seemingly paradoxical situation in which no data is personal from the outset and all data can become personal from the outset. (Janeček, 2018)

At the same time, as Della Corte correctly points out:

[a]scertaining whether data is personal frequently depends on each individual processing context and characteristics. The qualification of data as personal is contextual: the same piece of information can be anonymous in one moment in time and personal in another. As a result of the relative character of the notion of personal data, much is left to the discretion of the interpreter. (Della Corte, 2019)

In order to extend the material scope of the GDPR protection, synonyms ‘data’/‘information’ may be included in the definition of Article 4 of the GDPR, which in turn may provide protection for the most extensive area of personal information that can be obtained through the combination of non-personal or anonymous data. However, in this regard the blurring line between personal and non-personal data makes the GDPR “the law of everything” (Purtova, 2018), especially in the conditions when “[w]ith the advent of ever more performance data analysis techniques and hardware as well as the heightened availability of data points, it is becoming increasingly straightforward to relate data to natural persons” (Finck & Pallas, 2020).

In this context, the following question arises: if the right enshrined in Article 8 of the CFR protects personal information, regardless of its source, what does Article 7 of the CFR protect?

It is more acceptable to assume that the GDPR protects not the personal information, but the personal data itself. In its turn, the case-law of the ECtHR also shows that personal data itself is protected. In particular, the ECtHR indicates that human DNA or human cell samples contain a significant amount of unique personal data (*S. and Marper v. The United Kingdom* [2008]), and their mere retention without any further justification violates the right to private life under Article 8 of the ECHR. In other words, even storing of this data without any processing or interpretation already constitutes a violation of human fundamental rights. This practice makes it possible to say that there are two types of personal data that are not completely uniform in their internal nature: (1) the personal data that always contain personal information and any interpretation of it leads to

the identification of the data subject's identity, and (2) the personal data that does not have this intrinsic link with the person. If we assume that the protection of all personal data falls under the GDPR, which accepts the general concept of personal data without making a distinction between the personal data that contains personal information by default, and the data that does not, it is possible to argue that the protection provided by the GDPR does not protect the internal link between personal data and the person. It rather protects the data itself, behind which the person is "not visible". As Urgessa notes: "the existing data protection regime in the EU protects information that relates to us but does not, strictly speaking, protect us" (Urgessa, 2016).

Consequently, it is possible to say that this right provides an autonomous mode of using "personal data" without communication with a person. In its turn, the GDPR does not form the concept of a person's digital identity, but rather regulates the use of elements of this identity—the subjective dimension of a person that includes their habits or preferences, for which data is often processed. In other words, the GDPR does not proceed from the fact that personal data (or some of it) is a projection of the person. Meanwhile, this type of personal data is a component of personal identity, since "there is no difference between the information sphere of a person [interpreted by this internally personal data] and their personal identity" (Floridi, 2005). At the same time, the exploitation of this data is ethically burdensome and this is a kind of projection of the person, which requires stronger and more fundamental protection than can be achieved in the framework of the right to personal data protection.

## 6. Digital life and the emergence of the digital person (*homo digitalis*)

Protection of the person in the digital world is more than necessary, and it is more important than the protection of the personal data itself. The emergence of modern information technologies makes it possible to create a person's identity from its "digital parts" in favour of growing marketing practices. The creation of the person's digital profile is almost independent on his/her action or on providing his/her data by consent. In the conditions of non-transparency of data processing, the unlimited possibility of obtaining such data through the "consent myth" means consent to profiling, on the

one hand, and consent to the fragmentation of the digital self, on the other.

At the same time, the same information technologies have given a person the opportunity to project his/her identity in the digital space, for example, through the right to be forgotten. As Andrade points out: “The proposed conceptualization of the right to be forgotten not only makes sense from an identity point of view, it also contributes to the further development of the modern conception of identity, reinforcing its ‘anti-essentialistic’ understanding” (Andrade, 2012). Such projection involves creating representations of oneself in the digital space that reveal elements of one’s personality and personal life. With the creation of these ideas about oneself, the digital life of the person enters another aspect of human existence, which, although closely related to traditional life, is nevertheless characterized by specific interactions with other people.

Providing legal protection only for personal data, regardless of the protection of the individual itself, is in this case flawed: here, the personal data that make up a person’s digital life is not just data—it is the constituent elements of a digital person. “All data about us, in fact, are components of our personality,” as Rachel Richterich (2019) points out. Moreover, although the digital identity is outside of the biological body of the person, it is not outside of them. Human existence is no longer limited only to physical attributes, it also includes digital representations of these attributes. It reflects one of the modern anthropological discontinuities, connected with the human body, which until now was perceived as a “container” of identity and integrity of the person. Nowadays, in the context of the digital world, personal data itself has become such a “container”.

The dematerialization of the subject is not complete: it does not completely pass into another space-time continuum, and it is impossible to consider *res digitalis*—“a being that falls somewhere in the middle of physical existence and mind” (Kim, 2001). Rather this “digital self may reflect a physical self—albeit with distortions, edits and filters—and portable and even wearable technologies merge with or extend our physical bodies, generating continuous data related to our physicality in the world” (Kasket, 2019). The biological body does not disappear, but feelings, consciousness, action and will pass into the digital world. The life of a modern person is now developing in two different dimensions, which are interconnected as two sides of the same coin: they cannot be separated. This implies that it is impossible to legally protect one dimension and ignore the other one. The new dimension increases the pressure on the law, since the mass exchange of personal information that

occurred with the widespread introduction of the platform, along with “communication power”, gave individuals greater vulnerability.

If the physical existence of the person is established with fundamental rights to prevent any violation of his/her integrity, the emergence of the category of ‘digital person’ should lead to the emergence and recognition of rights, which should also protect his/her integrity in the digital world. Therefore, we should agree with the opinions of those researchers who point out that if people live digitally, it should be taken into account that their integrity extends to this dimension as well (Barbey, 2019). We believe that the existence of a digital person and digital life presupposes an expansion of the legal coordinates of the person and reveals the need to develop more comprehensive mechanisms for protection of the person in the digital world.

## 7. Right to digital integrity as the foundation for digital rights

Many researchers consider the emergence of the right to protect digital integrity to be a completely natural phenomenon. As Alexis Roussel points out: “If there is a right to physical integrity and to mental integrity, there must be a right to digital integrity. Exploiting someone’s personal data must be considered a violation of their digital integrity.” (Roussel, 2020) However, this position is fully consistent with the approach expressed by the UN that the rights which apply offline must also be protected online. Besides, in recent years, there have been a number of initiatives aimed at the adoption of the declarations of digital rights (e.g., Santini & Bensoussan, 2000; Barlow, 1996; etc.) and the recognition of the right to digital life, which should inevitably lead to the recognition of the right to digital integrity.

It should be mentioned that recognition of this right is not an end in itself, but it can solve quite practical problems in the field of human protection in the digital world. We tend to believe that recognition of the right to digital integrity in the CFR will legally establish a new relationship between the person and his/her personal data, and will help consolidate the position that personal data has an inherent connection with the person themselves at a higher legislative level. At the same time, it is necessary to note that the main premise of the existing legislative acts of the EU, *inter alia* the GDPR, is basically the assumption that personal data is a danger to the person themselves, and the person is a potential victim of the actions of

the data processors. In this context, the following question arises: Where did this perception of the dangers associated with the use of personal data come from? We argue that it is from the idea that their use can lead to manipulation of the identity of the data subject. Thus, recognition of the right to digital integrity, among other things, will strengthen the direction of the will of the EU legislator.

Creating or choosing one's own content of one's digital identity involves providing the person with those legal instruments through which they are ensured such creation and protection of their choice. To paraphrase Benn (1984), who points out that if an individual is confident that they can be themselves, they can believe in themselves as the person, it is possible to say that the law should provide the person with the confidence that they can be the person they choose to be. In this sense, the person is a subject who is aware of themselves as an agent, choosing and trying to manage their own course in the digital world.

Recognition of digital integrity as a new fundamental right within the framework of the right to personal integrity implies some change in the recognized "legal paradigm" that we see in the CFR, according to which the wording of Article 3 implies the existence of a "negative right", aimed at protecting the human body from any "unauthorized" interference from outside. However, the right to digital integrity itself will not help protect the person's "digital identity" from unauthorized intrusion. The right to the digital integrity of the individual must be considered in close relationship with the right to personal self-determination and should provide an opportunity for the person to exercise his/her positive right to informational self-determination, i.e. to determine without coercion what information or data as "building blocks" will form his/her digital identity, "which information about him is and will be available and accessible" (Buitelaar, 2017), as well as maintain and control what will be his/her reputation, dignity and integrity.

From the above-mentioned perspective, the right of each person to create their own digital privacy perimeter could be a new perspective on recognizing the right to digital integrity as a basis for informational self-determination. As one knows, the GDPR states that individuals must have control over their personal data, and lays the foundation for the recognition of the right to informational self-determination, the content of which can be defined through the GDPR-rights, i.e., the rights to be informed, erasure, rectification, access, object, restrict processing, data portability and not to be

subject to a decision based solely on automated processing. We believe that the recognition of the digital integrity of the person as a fundamental right will mean laying a new foundation for the rights provided in the GDPR and form the basis for the concept of the digital identity of the person.

Moreover, even in its case-law, the CJEU reflects on digital rights and, *inter alia*, on the right to be forgotten as a certain focus on the assumption of the possibility of “managing” a digital person. In particular, in the judgment of the CJEU against Google (*Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014]), the person is granted with the right to revoke a link from search engines. As one can see, this judgment gives the person a tool that allows them to control his/her digital person. Thus, everyone can simulate his/her projection in the digital world by requesting the removal of the search engine index that is considered to be inadequate. Thus, the right to de-indexation, or the “right to be forgotten” becomes one of the tools for the formation of digital integrity. In this case, informational self-determination becomes the right about when and within what limits information that constitutes the person’s unique identity and integrity should be disclosed to others.

Although the recognition of the right to digital integrity will also strengthen the ability to exercise self-determination through digital rights, a person nevertheless, as it was already noted, cannot realize the full exercise of the right to self-determination in the traditional legal aspect: this is practically impossible, especially because of the parties’ imbalance, which weakens the “informed” nature of the consent of the data subject. In addition, the consent rules in the GDPR are only one of the conditions for the legitimate processing of personal data, among which, according to Article 8(2) of the CFR, there are any other “legitimate basis laid down by law”. The extension of the GDPR rights to the circumstances of using the person’s personal attributes, identity and integrity without his/her consent, but for legitimate reasons, makes it possible to easily extract information that is an element of personality and consider it as a commodity. This practice will further facilitate profiling, which is now one of the keys to business. Simultaneously, even if we assume that such self-determination is still possible, the following questions arise: How appropriate is it to grant the person such a right without special restrictions regarding his/her “digital body” as an extension of the person? If these restrictions are still necessary, what mechanism can limit the role of the market and autonomy in the modern conceptual framework? As noted, the main premise of the GDPR is the assumption that personal data is a danger to the person themselves.

However, nowadays the person themselves no longer sees such a danger. Moreover, they disclose this data for the implementation of their digital life. No matter how paternalistic it may sound, in our opinion, the legal mechanisms in the digital world should also protect people from themselves. Some researchers believe that the mechanism limiting autonomy and the market should be sought in the legislation regulating the “biological world”. In particular, as de Hingh and Lodder (2020) point out: “The legal status of the human body parts does not correspond with the status of personal data entirely, but there are good grounds to make the comparison”.

Thus, if we postulate that our digital body should be regulated as a physical body, then violations of human dignity become obvious: we see a gap, distribution and appropriation of the person, contrary to the traditional humanistic approach. This development requires a mechanism that struggles with the separation of parts of the person or his/her identity from himself/herself. In this case, the unrestricted right over personal data is out of the question.

## 8. Digital integrity as a new manifestation of human dignity

The laws of the biological world have restrictions for disposing of personal attributes. As Andorno notes:

The notion of human dignity is beginning to be seen as the last barrier against the alteration of some basic features of the human species [...]. It should be noted that resorting to human rights is insufficient to cope with these new challenges [...] as a threat, not to individuals, but to the integrity of the human species as such [...]. This is the reason why the 1997 Universal Declaration on the Human Genome and Human Rights directly appeals to the notion of human dignity, not to human rights [...]. (Andorno, 2009)

These laws are limiting the autonomy of the person through a restraining dimension of human dignity in bio-law, which prohibits turning elements of the human body into goods, which is actually the meaning of the ‘restrictive concept of human dignity’. In this regard, Beyleveld and Brownsword point out that there are

two opposed conceptions, ‘human dignity as empowerment’, which treats human rights as based on the intrinsic dignity of humans, identified

with individual autonomy, and ‘human dignity as constraint’, which acts as an umbrella for a number of duty-driven approaches. While viewing human dignity primarily as empowerment, the authors argue that it is not autonomy as such, but vulnerable agency around which dignity as the basis of human rights is [...] analyzed. (Beyleveld & Brownsword, 2001, p. 11)

We believe that the right to digital integrity should be understood from the perspective of ‘human dignity as constraint’ to be able to effectively ensure the protection of the person’s identity in the digital world and restrain the process of commodification of his/her personal data.

Moreover, in *Netherlands v. Parliament and Council* [2001], the CJEU recognizes the existence of one fundamental right of dignity and integrity. In particular, paragraph 70 of the judgment states: “It is for the Court of Justice, in its review of the compatibility of acts of the institutions with the general principles of Community law, to ensure that the fundamental right to human dignity and integrity is observed”. Although in the paragraph of the judgment the word ‘and’ was inserted between the words ‘*dignity*’ and ‘*integrity*’, suggesting that they reflect two different values or concepts, nevertheless it is assumed that dignity was seen as standing for the claim that the protection of the person’s physical and psychological integrity is a justification for their humanity.

We believe that the relationship between ‘*dignity*’ and ‘*integrity*’, specified in the above case, does not seem random. The ambiguity of the concept of ‘dignity’, which is used to get contradictory results in support of opposing positions on the same issue, is a well-known phenomenon, but their emphasized significance for legal discourse leads to the need to search for its content. Awareness of the obvious futility of searching for the unambiguous content of dignity in philosophical discourse implies the disclosure of the content of this concept through its consideration in connection with personal integrity. This manifestation of “human dignity pragmatism” (in the terminology of Addis (2015)) consists in identifying the idea of dignity from the practice of human rights, as well as from the choices and decisions that are made in the name of dignity. In this regard, as one can see, the CFR in its articles reduces dignity to four utilitarian positions of human rights: (1) the right to life; (2) the right to integrity of the person; (3) the inadmissibility of torture; and (4) the prohibition of slavery, which are mostly formulated as prohibitions. These prohibitions, while protecting dignity by pointing out the types of behaviour that are “unworthy”, at the same time at least protect

the physical and psychological aspects of the integrity of the person, which is necessary for the existence of the person, and the violation of which means the denial of recognition of the person. Such prohibitions are related to the need to protect the integrity of the person, whose body is vulnerable and, as Michel Foucault (1975) points out, it can become the target of a force that can be controlled and produced for certain functions.

Considering the concept of dignity in relation to the concept of personal integrity makes it an immanent quality of human personality. We can cautiously come to the conclusion that the idea of dignity, especially in its restrictive version ('human dignity as constraint'), that Beyleveld and Brownsword are talking about in their research (Beyleveld & Brownsword, 2001), insists on protecting personal integrity. As we mentioned above, the limited concept is more protective for the person when there is a threat of a violation of personal integrity in the interests of third parties: it will help avoid pressure on the person to give up aspects of their personality. The research of van Beers (2009) has shown that the principle of human dignity ultimately forms the basis for protection against the risks of commercialization, instrumentalization and dehumanization of human beings.

Human dignity is even more important in the given aspect because it also protects those who do not have full self-determination. The legal category that has such a significant potential can be crucial for the personal data protection. As Mittelstadt and Floridi (2016, p. 471) point out: "It is likely more ethically problematic to strip context from data used to track the behaviours of individuals than it is to remove identifying information to tissue samples for medical research". "Digital ICT's can increase informational privacy" and change the "very nature of privacy" (Floridi, 2005), which is "nothing less than the defence of the personal integrity of the packet of information" (i.e., the individuals) and that an invasion of an individual's informational privacy is a "disruption of the informational environment that it constitutes". According to Floridi, violation of privacy "is not a violation of ownership, of personal rights", but instead "a violation of the nature of information itself". So in Floridi's account, a violation of privacy is not tied to an agent's personal rights (e.g., the right involving control and ownership of information), and is rather linked to conditions affecting that information environment that the agent constitutes. He concludes that a breach of one's informational privacy is "a form of aggression towards one's personal identity" (Floridi, 2005). The digital body, in this case, is considered as a kind of extension of the person, which must be constantly "monitored" to ensure its proper functioning.

In Floridi's reasoning, the body–information dichotomy that underlies the separate legal regulation of the body and personal data is lost—a cardinal step, for which the EU law, in our opinion, is not yet ready. In this context, the following question arises: what will prevent the same positions of “human dignity pragmatism” to indicate the manipulation of the individual through its “digital components” as another “unworthy” behaviour? Nothing will. On the contrary, it will also help to implement the restrictive concept of human dignity to constrain the market, which is not new for the EU law.

It has already been reflected once in the case-law of the CJEU, in the so-called *Omega* ruling, to resolve the tension between respect for human dignity (constructed as part of public policy) and the freedom of goods and services (*Omega Spielhallen- und Automatenaufstellungs-GmbH v. Oberbürgermeisterin der Bundesstadt Bonn* [2004]). As human dignity is the general principle of law and the fundamental basis of the public policy for restriction of the freedom of services, “the Community legal order undeniably strives to ensure respect for human dignity as a general principle of law” (*Omega Spielhallen- und Automatenaufstellungs-GmbH v. Oberbürgermeisterin der Bundesstadt Bonn* [2004]). Evidently, the CJEU identified it as a new imperative of the EU legal order in addition to four freedoms, but, unfortunately, this approach was revised.

However, it should be noted that, after the adoption of the Lisbon Treaty, which gave the CFR the role of the EU's primary law, the CFR begins to play a special role. Among others, in referral to the area of freedom, security and justice in the Preamble of the CFR and, in particular, the fact that the EU has an intention to put the individual at the centre of its activities (Preamble of the Charter of Fundamental Rights of the European Union, 2000/C 364/01). This means a new round of rethinking the balance between freedoms and human dignity, especially in its restrictive concept.

In recent years, EU's attention has shifted from market-oriented aspects of personal data protection to more valuable ones, although so far only in the sphere of ethical developments. For instance, the EDPS Opinion 4/2015, *Towards a New Digital Ethics: Data, Dignity and Technology* states that “the right to data protection was originally conceived in the 1970s and 80s as a way of compensating the potential for the erosion of privacy and dignity through large scale personal data processing” (EDPS, 2015, p. 12; see also Nussbaum, 1995). “Violations of dignity may include objectification, where a person is treated as a tool serving someone else's purposes” (EDPS, 2015, p. 12). At the same time, the Opinion did not consider the possibility of using

human dignity as a constraint for personal autonomy or the market. The report *Towards a Digital Ethics* of the Ethics Advisory Group (hereinafter the EAG) focused on the need to make technology work in the interests of human dignity (EDPS, 2018) and gave a conclusion that “the fundamental values underlying European data protection and other fundamental rights and freedoms must be re-affirmed” (EDPS, 2018). The EAG makes some references to the restrictive concept of human dignity. Speaking about the problem of commercialization of personal data, it points out that “when people are considered not as individuals, but as simple temporary aggregates of data processed on an industrial scale for optimization [...] by interacting with them, they may not be fully respected either in their dignity or in their humanity”(EDPS, 2018).

Besides, in 2018, the European Commission issued the Communication on the Artificial Intelligence for Europe (COM (2018)237 final), which indicates the intention to develop draft guidelines on AI ethics with due regard to the Charter of Fundamental Rights of the European Union (Communication COM (2018)237 final). In the same year, the international conference of data protection and privacy commissioners, held in Brussels, published the Declaration on Ethics and Data Protection in Artificial Intelligence, which states that:

The 40<sup>th</sup> International Conference of Data Protection and Privacy Commissioners considers that any creation, development and use of artificial intelligence systems shall fully respect human rights, particularly the rights to the protection of personal data and to privacy, as well as human dignity, non-discrimination and fundamental values, and shall provide solutions to allow individuals to maintain control and understanding of artificial intelligence systems (Declaration on Ethics and Data Protection in Artificial Intelligence, 2018).

Thus, ethical developments in the EU indicate a possible, preferred direction for the further regulation of personal data protection in the context of the restrictive concept of human dignity, which implies the recognition of digital integrity as a new fundamental right within the framework of the right to personal integrity. Although time will tell whether the EU legislator will move in this direction (Andraško & Mesarčík, 2021).

## 9. Conclusion

As a result of our research, we came to the conclusion that now the right of personal data itself cannot effectively protect personal data as a component of personal identity in the EU. The modern legislative consolidation of the right to personal data protection provides an autonomous mode of using personal data without communication with the person. The GDPR rather protects the data itself, but not the person, since it does not form the concept of a person's digital identity, and instead regulates the use of elements of that identity—the subjective dimension of a person that includes their habits, preferences, for which data are often processed. In other words, the GDPR does not proceed from the fact that personal data is a component of personal identity.

Meanwhile, the use of personal data can be ethically burdensome and, therefore, requires stronger and fundamental protection than can be achieved within the framework of the right to personal data protection. The fundamental basis should more effectively prevent the process of turning an individual into a commodity with the help of their personal data—the legal protection of personal data, especially in the GDPR, is formulated in accordance with the rules inherent in property relations. We believe that personal data cannot be effectively protected in the context of the regulation of an independent fundamental right to personal data protection, implemented through GDPR. In these conditions, it is necessary to find an alternative foundation for the legal regulation and protection of personal data. We consider that the right to digital integrity can be a new foundation for digital rights, the recognition of which, similar to the right to physical and psychological integrity, can protect the person from becoming a commodity and reduce the number of cases of violation of human dignity in the digital sphere.

Considering digital integrity as a basis for regulating the sphere of personal data protection is justified by the fact that it can protect the person, even if the latter does not know about the existence of their digital applications. A person should not only be able to control information about himself/herself using digital rights, but also be sure that if such control is not completely possible, no one will extract, transfer or use his/her information to harm him/her, even in the case of his/her consent. In this context, the EU needs a new regulatory framework based on a moderate restrictive data protection regime. The recognition of digital integrity as the basis of digital rights

and as a new manifestation of the restrictive concept of human dignity will help increase the level of effective protection of the individual in the digital sphere and weaken the existing trend of recognizing the right of ownership of personal data. In this case, the digital body is considered as a kind of continuation of a person, which must be constantly “monitored” to ensure its proper functioning.

It should be noted that, in recent years, the EU’s attention has shifted from the market aspects of personal data protection to more valuable ones, although so far only in the field of ethical developments. Such ethical changes in the EU indicate a possible and preferred direction for further regulation of personal data protection in the context of the restrictive concept of human dignity, which implies the recognition of digital integrity as a new fundamental right.

## Acknowledgment

The article was prepared as part of the projects IGA\_PF\_2021\_014 ‘Tackling the Protection of the Right to Personal Integrity and Body-Derived Data in Information Society: New Challenges for EU Law’ (Lusine Vardanyan), and GAČR no. 20-27227S ‘The Advent, Pitfalls and Limits of Digital Sovereignty of the European Union’, funded by the Czech Science Foundation (Václav Stehlík, Hovsep Kocharyan).

**Lusine Vardanyan** is a PhD researcher at the Department of International and European Law (Faculty of Law, Palacký University in Olomouc). In her research, she focuses on the problematic aspects of personal data protection in EU law.

**Václav Stehlík** is an associate professor of EU law at the Department of International and European Law (Faculty of Law, Palacký University in Olomouc). In his research, he focuses on EU internal market, migration law and EU law enforcement issues.

**Hovsep Kocharyan** is a PhD researcher at the Department of International and European Law (Faculty of Law, Palacký University in Olomouc). In his research, he focuses on the contemporary challenges of data and privacy protection in EU law.

## References

- A European Strategy for Data (2020), Communications from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee and the Committee of the regions, COM (2020)66 final, 19.2.2020. Retrieved from [https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020\\_en.pdf](https://ec.europa.eu/info/sites/info/files/communication-european-strategy-data-19feb2020_en.pdf) [accessed Apr 2022]
- Addis, A.** (2015), 'Human dignity in comparative constitutional context: In search of an overlapping consensus,' *Tulane Public Law Research Paper*, no. 15-11.
- A Digital Single Market Strategy for Europe (2015), Analysis and Evidence Accompanying the document Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM (2015)192 final, SWD (2015) 100 final, 6.5.2015. Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015SC0100&rid=1> [accessed Apr 2022]
- Andorno, R.** (2009), 'Human dignity and human rights as a common ground for a global bioethics,' *The Journal of Medicine and Philosophy: A Forum for Bioethics and Philosophy of Medicine*, vol. 34, no. 3, pp. 223–240. <https://doi.org/10.1093/jmp/jhp023>
- Andraško, J. & Mesarčik, M.** (2021), 'Those who shall be identified: The data protection aspects of the legal framework for electronic identification in the European Union,' *TalTech Journal of European Studies*, vol. 11, no. 2, pp. 3–24. <https://doi.org/10.2478/bjes-2021-0012>
- Artificial Intelligence for Europe (2018), Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, COM (2018)237 final, 25.4.2018.
- Barbey, G.** (2019), 'Il est temps de reconnaître l'intégrité numérique des individus,' *Le Temps*, 25 January.
- Barlow, J. P.** (1996), 'A Declaration of the Independence of Cyberspace,' *Electronic Frontier Foundation*. Retrieved from <https://www EFF.org/cyberspace-independence> [accessed Apr 2022]
- Becerill, A.** (2018), 'The value of our personal data in the Big Data and the Internet of All Things Era,' *ADCAIJ: Advances in Distributed Computing and Artificial Intelligence Journal*, vol. 7, no. 2, pp. 71–79. <https://doi.org/10.14201/ADCAIJ2018727180>
- Benn, S. I.** (1984), 'Privacy, freedom, and respect for persons,' in F. D. Schoeman (ed.) *Philosophical Dimensions of Privacy: An Anthology*, Cambridge: Cambridge University Press, pp. 223–244. <https://doi.org/10.1017/CBO9780511625138.009>

- Beyleveld, D. & Brownsword, R.** (2001), *Human Dignity in Bioethics and Biolaw*, Oxford: Oxford University Press.
- CJEU (2017), Press Release no. 84/17 Luxembourg, Opinion 1/15, Court of Justice of the European Union, 26.7.2017. Retrieved from <https://curia.europa.eu/jcms/upload/docs/application/pdf/2017-07/cp170084en.pdf> [accessed Apr 2022]
- Declaration on Ethics and Data Protection in Artificial Intelligence (2018), 40th International Conference of Data Protection and Privacy Commissioners, Brussels. Retrieved from [http://globalprivacyassembly.org/wp-content/uploads/2019/04/20180922\\_ICDPPC-40th\\_AI-Declaration\\_ADOPTED.pdf](http://globalprivacyassembly.org/wp-content/uploads/2019/04/20180922_ICDPPC-40th_AI-Declaration_ADOPTED.pdf) [accessed Apr 2022]
- De Franceschi, A. & Lehmann, M.** (2015), 'Data as tradeable commodity and new measures for their protection,' *The Italian Law Journal*, vol. 1, no. 1, pp. 51–72.
- de Hingh, A. & Lodder, A. R.** (2020, forthcoming), 'The role of human dignity in processing (health) data building on the organ trade prohibition,' in T. Synodinou, Ph. Jogleux, Ch. Markou & Th. Prastitou (eds.) *EU Internet Law in The Digital Era*, Springer. Available at <https://ssrn.com/abstract=3453302>. [https://doi.org/10.1007/978-3-030-25579-4\\_12](https://doi.org/10.1007/978-3-030-25579-4_12)
- Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources and Others and Kärntner Landesregierung and Others* [2014], CJEU Joined cases C 293/12 and C 594/12, ECLI:EU:C:2014:238, 8.4.2014.
- EDPS (2015), Opinion 4/2015, *Towards a New Digital Ethics: Data, Dignity and Technology*, European Data Protection Supervisor, September 2015. Retrieved from [https://edps.europa.eu/sites/edp/files/publication/15-09-11\\_data\\_ethics\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/15-09-11_data_ethics_en.pdf) [accessed Apr 2022]
- European Commission (n.d.), 'Data protection in the EU.' Retrieved from [https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu\\_en](https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_en) [accessed Apr 2022]
- Floridi, L.** (2005), 'The ontological interpretation of informational privacy,' *Ethics and Information Technology*, vol. 7, pp. 185–200. <https://doi.org/10.1007/s10676-006-0001-7>
- Foucault, M.** (1975), *The Birth of the Clinic: An Archaeology of Medical Perception*, transl. by A. M. Sheridan Smith, New York: Vintage Books.
- František Ryneš v. Úřad pro ochranu osobních údajů* [2014], CJEU Case C212/13; ECLI:EU:C:2014:2428, 11.12.2014.
- Google Spain SL, Google Inc. v. Agencia Española de Protección de Datos (AEPD), Mario Costeja González* [2014], CJEU Case C131/12, ECLI:EU:C:2014:317, 13.5.2014.
- Hamulák, O.; Kiss, L.; Gábriš, T. & Kocharyan, H.** (2021), "“This content is not available in your country”: A general summary on geo-blocking in and outside the European Union,' *International and Comparative Law Review*, vol. 21,

- no. 1, pp. 153–183. <https://doi.org/10.2478/iclr-2021-0006>
- Janeček, V.** (2018), 'Ownership of personal data in the Internet of Things,' *Computer Law & Security Review*, vol. 34, no. 5, pp. 1039–1052.  
<https://doi.org/10.1016/j.clsr.2018.04.007>
- Ježová, D.** (2020), 'Sharing economy in digital single market: EU—a phenomena with future potential,' *European Studies: The Review of European Law, Economics and Politics*, vol. 7, pp. 218–236.
- J. Nold, Kohlen- und Baustoffgroßhandlung v. Commission of the European Communities* [1975], CJEU Case 4-73, ECLI:EU:C:1974:51, 14.5.1975.
- Joamets, K. & Chochia, A.** (2020), 'Artificial intelligence and its impact on labour relations in Estonia,' *Slovak Journal of Political Sciences*, vol. 20, no. 2, pp. 255–277. <https://doi.org/10.34135/sjps.200204>
- Joamets, K. & Chochia, A.** (2021), 'Access to artificial intelligence for persons with disabilities: Legal and ethical questions concerning the application of trustworthy AI,' *Acta Baltica Historiae et Philosophiae Scientiarum*, vol. 9, no. 1, pp. 51–66. <https://doi.org/10.11590/abhps.2021.1.04>
- Kasket, E.** (2019), 'Mourning and memorialization on social media,' in A. Attrill-Smith, C. Fullwood, M. Keep & D. J. Kuss (eds.) *The Oxford Handbook of Cyberpsychology*, Oxford: Oxford University Press.  
<https://doi.org/10.1093/oxfordhb/9780198812746.013.26>
- Kerikmäe, T.; Hamulák, O. & Chochia, A.** (2016), 'A historical study of contemporary human rights: Deviation or extinction?' *Acta Baltica Historiae et Philosophiae Scientiarum*, vol. 4, no. 2, pp. 98–115. <https://doi.org/10.11590/abhps.2016.2.06>.
- Kim, J.** (2001), 'Phenomenology of digital-being, *Human Studies*,' vol. 24, pp. 87–111.  
<https://doi.org/10.1023/A:1010763028785>
- Kocharyan, H.; Vardanyan, L.; Hamulák, O. & Kerikmäe, T.** (2021), 'Critical views on the right to be forgotten after the entry into force of the GDPR: Is it able to effectively ensure our privacy?' *International and Comparative Law Review*, vol. 21, no. 2, pp. 96–115. <https://doi.org/10.2478/iclr-2021-0015>
- Malgieri, G.** (2016), 'Property and (intellectual) ownership of consumers' information: A new taxonomy for personal data,' *Privacy in Germany*, vol. 4.  
<https://doi.org/10.37307/j.2196-9817.2016.04.05>
- Maximillian Schrems v. Data Protection Commissioner* [2015], CJEU Case C-362/14; ECLI:EU:C:2015:650, 6.10.2015.
- Mittelstadt, B. D. & Floridi, L.** (2016), *The Ethics of Biomedical Big Data*, Cham: Springer. <https://doi.org/10.1007/978-3-319-33525-4>
- Monti, A. & Wacks R.** (2019), *Protecting Personal Information: The Right to Privacy Reconsidered*, Oxford: Hart Publishing. <https://doi.org/10.5040/9781509924882>

- Nussbaum, M.** (1995), 'Objectification,' *Philosophy and Public Affairs*, vol. 24, no. 4, pp. 249–291. <https://doi.org/10.1111/j.1088-4963.1995.tb00032.x>
- Ohm, P.** (2010), 'Broken promises of privacy: Responding to the surprising failure of anonymization,' *UCLA Law Review*, vol. 57, pp. 1701–1777.
- Omega Spielhallen- und Automatenaufstellungs-GmbH v. Oberbürgermeisterin der Bundesstadt Bonn* [2004], CJEU Case C-36/02, ECLI:EU:C:2004:614, 4.10.2004.
- Purtova, N.** (2018), 'The law of everything. Broad concept of personal data and future of EU data protection law,' *Law, Innovation and Technology*, vol. 10, no. 1, pp. 40–81. <https://doi.org/10.1080/17579961.2018.1452176>
- Rechnungshof (C-465/00) v. Österreichischer Rundfunk and Others and Christa Neukomm (C-138/01) and Joseph Lauerermann (C-139/01) v. Österreichischer Rundfunk* [2003], CJEU Joined cases C-465/00, C-138/01 and C-139/01, ECLI:EU:C:2003:294, 20.5.2003.
- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L* 119, 4.5.2016, pp. 1–88.
- Richterich, R.** (2019), 'L'intégrité numérique: le vrai combat pour nos données,' *Le Temps*, 11 January.
- Roussel, A.** (2020), 'The right to digital integrity of the human person,' *Digitale Bürger\*innrechte*, 21 February. Retrieved from <https://www.fabrikzeitung.ch/the-right-to-digital-integrity-of-the-human-person/#/> [accessed Apr 2022]
- S. and Marper v. The United Kingdom* [2008], Applications nos. 30562/04 and 30566/04, European Court of Human Rights, 4.12.2008, p. 75.
- Santini, A. & Bensoussan, A.** (2000), 'Livre blanc sur les droits de l'homme numérique.' Retrieved from <https://www.alain-bensoussan.com/wp-content/uploads/39889121.pdf> [accessed Apr 2022]
- Schwartz, P. & Solove, D.** (2011), 'The PII problem: Privacy and a new concept of personally identifiable information,' *New York University Law Review*, vol. 86, pp. 1814–1898.
- Sweeney, L.** (2000), *Simple Demographics Often Identify People Uniquely*, Carnegie Mellon University, Data Privacy Working Paper 3.
- Tietosuojaalvaututettu v. Satakunnan Markkinapörssi Oy and Satamedia Oy* [2008], CJEU Case C-73/07: ECLI:EU:C:2008:727, 16.12.2008.
- Urgessa, W. G.** (2016), 'The feasibility of applying EU data protection law to biological materials: Challenging 'data' as exclusively informational,' *JIPITEC: Journal of Intellectual Property, Information Technology and Electronic Commerce Law*, vol. 7, no. 2, pp. 96–109. <https://doi.org/10.2139/ssrn.2840764>
- van Beers, B. C.** (2009), *Persoon en Lichaam in het Recht. Menselijkewaardigheid en zelfbeschikking in het tijdperk van de medischebiotechnologie*, PhD thesis, Vrije Universiteit Amsterdam.

- van der Sloot, B.** (2017), 'Legal fundamentalism: Is data protection really a fundamental right?' in R. Leenes, R. van Brakel, S. Gutwirth & P. De Hert (eds.) *Data Protection and Privacy: (In)visibilities and Infrastructures*, Cham: Springer, pp. 3–30. [https://doi.org/10.1007/978-3-319-50796-5\\_1](https://doi.org/10.1007/978-3-319-50796-5_1)
- Vardanyan, L. & Stehlík, V.** (2020), 'Is the case law of ECtHR ready to prevent the expansion of mass surveillance in post-COVID Europe?' *European Studies*, vol. 7, pp. 253–272.