The role of human dignity in processing (health) data building on the organ trade prohibition

de Hingh, Anne; Lodder, Arno R.

published in
EU Internet Law in the Digital Era
2020

DOI (link to publisher)
10.1007/978-3-030-25579-4_12

document version
Publisher's PDF, also known as Version of record

Chapter 12
The Role of Human Dignity in Processing (Health) Data Building on the Organ Trade Prohibition

Anne E. de Hingh and Arno R. Lodder

Abstract The datafication, commodification, and commercialization of our existence as an inevitable part of the online infrastructure of today not only affects our privacy but it goes deeper by touching upon even more fundamental conditions of being human. In this chapter, bio-medical regulations prohibiting the trade of human body parts are explored to see whether the non-commercialization principle in these laws is helpful in assessing data processing practices. An analogy between data processing and organ trade may help us to develop a new perspective on what constitutes improper commercial use of personal data and find ways to prohibit (reprehensible aspects of) the trade in personal data. We propose to reorient the debate on data processing by introducing the notion of human dignity as constraint into the discussion. A prohibition of personal data commercialism (analogous to a prohibition of transplant commercialism) could contribute to a more future-proof regulation of data processing activities.

1 Introduction

The effects of harvesting personal data by large commercial entities, such as internet companies, social media, and internet service providers, are at least threefold. First, virtually all aspects of our lives are converted into computerized data (datafication, see e.g. Newell and Marabelli 2015). Subsequently, our identities, habits, and behavior are transformed into new forms of value or commodities (commodification, see e.g. Schwartz 2004). Finally, as our personal data and consumer profiles represent high values, they are purchased, processed, and sold on over and over again (commercialization, see e.g. Smutny et al. 2017). The worldwide data broker industry, which thrives on the fact that personal data generate economic value, makes for great revenues.[1]

[1] OECD (2013).

A. E. de Hingh · A. R. Lodder (✉)
CLI-Center for Law and Internet, Vrije Universiteit Amsterdam, Amsterdam, The Netherlands
e-mail: a.r.lodder@vu.nl

T.-E. Synodinou et al. (eds.), *EU Internet Law in the Digital Era*,
https://doi.org/10.1007/978-3-030-25579-4_12

The datafication, commodification, and commercialization of our existence as an inevitable part of the online infrastructure of today not only affects our privacy but it goes deeper by touching upon even more fundamental conditions of being human. In this chapter, bio-medical regulations prohibiting the trade of human body parts are explored to see whether the non-commercialization principle in these laws is helpful in assessing data processing practices. An analogy between data processing and organ trade may help us to develop a new perspective on what constitutes improper commercial use of personal data and find ways to prohibit (reprehensible aspects of) the trade in personal data.

There is another reason for our approach. Since the nineteenth century, the world is connected via telex, telephony, fax, and most recently, computers. This latter network, of connected computers, known as the internet, is gradually moving into a next phase. Besides PCs and from later date smartphones and tablets, presently all kinds of objects, such as toothbrushes, wearables, TVs and cameras, are connected to the internet. The internet of bodies is a subspecies of this internet of things, and represents the connected body. This internet of bodies facilitates communication about, e.g. the performance of implants, as well as the health condition of the individual being monitored. Moreover, pace makers can be connected, insulin levels can be measured at a distance, eventually followed by automatic injections. All kinds of sensitive data are communicated about a person's health, like general condition, heartbeat, blood pressure, etc.

Now the processing of data gets close to and even enters our bodies, Article 3(2) of the EU Charter springs to mind: "the prohibition on making the human body and its parts as such a source of financial gain". This article was not drafted with data processing in mind, but covers, e.g. slavery and human trafficking in relation to the body and its parts. One could, however, argue that the data being transferred from human implants and wearables is in conflict with this fundamental right. Companies are making money with parts of the human body, viz. data (in)directly related to our body. More generally, one could question to what extent human dignity asks for protection against the processing of (health) data. Hence, Article 1 of the EU Charter of Fundamental Rights does state "Human dignity is inviolable. It must be respected and protected."

In relation to trade in body parts, governments set limits to the free choice of its citizens, even in criminal law. In May 2015, Marc H. put an advertisement on Marktplaats.nl, the Dutch eBay, to sell his kidney for the sum of 50,000 euros. He was arrested by the police soon afterwards but acquitted because of insufficient evidence for financial gain. As the suspect had not yet received any offer, the purpose of financial gain could not be sufficiently demonstrated—advertising body parts alone was considered insufficient evidence for the purpose of financial gain. In this chapter, we do not focus on eventual sanctions, be it criminal, administrative, or civil, but explore the underlying principles for regulating the processing of (health) data.

The chapter is structured as follows. In the light of the focus of our chapter (an analogy between data processing and the organ trade prohibition), we discuss some relevant assumptions of data protection law. Subsequently, the analogy between

data processing and trade in body parts is explored. We aim to strengthen our observations related to the analogy between trade in body parts and data processing in general with a discussion of the processing of health data, and briefly touch upon paternalism (Husak 2009).

2 Need for a Change in Application of Data Protection Law

The topic of this paper is part of a broader argument in the context of data protection law (Bygrave 2018). Our concern with data protection law, not only relates to the fact that gradually more intimate data is being processed. This is actually one side of the spectrum, the processing of (very) sensitive data. This is what the GDPR does, to some extent, regulate, because in principle it is not allowed to process special categories of data such as health data (Article 9(1) GDPR). However, there are exceptions to this rule, e.g. in case the data were manifestly made public by the data subject (Article 9(2)(e) GDPR). The other end of the spectrum is personal data to which data processing rules apply, but where one can question whether data protection law for these data is necessary in the first place. We start this chapter by briefly discussing what we would like to call different flavors of data processing.

Many observe the discrepancy between the scope of GDPR norms and the effect these norms have in practice. We believe that data protection law, as it exists today, is too straightforwardly simple. The GDPR distinguishes special categories of data, but besides that the same norms apply to a controller/processor not interested at all in the personal data that are being processed (e.g. ERP cloud providers), controllers who have a small business and only use personal data to deliver goods, controllers whose business model is based on data analytics, etc. A possible reason might be that the drafters of the norms do not provide the data protection law framework with empirical backing, cf. Bamberger and Mulligan (2015):

> This absence of empirical assessment of regulatory impact on the practice of privacy leaves legal reformers shooting in the dark, without a real understanding of the ways in which previous regulatory attempts have either promoted or thwarted privacy's protection.

What is happening right now is that big data processors like Facebook and Google largely can continue with their business as usual, whereas all kind of small players like sport clubs, schools, stores, are outright panicking about the consequences of the GDPR, in this context commonly referred to as "The new privacy law". Also in academia, there is a tendency to ask for permission of processing of totally innocent use, e.g. asking permission to a group of 15 people in the same room, for the same reasons, to share the e-mail addresses—funny enough they already did when sending the invitation…

Thus, the data protection norms that apply to Google, Facebook, and the likes are the same as those that apply to the next corner butcher and flower shop or the cloud provider only providing the tech to process data cannot be left unnoticed. A physical analogy for the latter situation is that the company that stores boxes with personal

data is controller/processor. We want to start a discussion on differentiation of data processing regimes. What we propose is tentative, and is meant as a starting position rather than a well worked out division. We suggest to distinguish the following four categories, ranging from most infringing (1) to hardly infringing if at all:

1. Processing is in principle forbidden, but the DPA can license the processing activity. One category might be the processing of health data for commercial purposes. Article 9(2)(a) GDPR provides this option to Member States, to allow data subject to lift the prohibition of processing as defined in Article 9(1) GDPR. Markou (2011) did propose a ban for the processing of sensitive data in the context of commercial profiling and personalized advertising. Sometimes processing of health data is inevitable, e.g., for insurance companies. They will thus get a license. A more controversial category is to prohibit the business model that is solely based on the processing of personal data.
2. The current framework. The GDPR as it is right now should apply to all data processing activities that do not fall under one of the other categories.
3. GDPR light. A basic set of rules, based on Article 5 GDPR. An organization needs to demonstrate that they act in accordance with the data protection principles listed in Article 5. This category applies based on for what purpose the data is being processed, and the nature and number of data being processed.
4. Processing is allowed, but security measures must be taken. This category applies to parties processing data as a service (e.g. cloud providers), and do nothing with the data other than storing the data or providing the services necessary to process the data.

We suggest the data protection framework, or at least its application, should better consider the nature of the data and the purpose for which the data is being processed along the lines just sketched. We do not further elaborate on this topic in this paper in general, but as a first step concentrate on how the data protection norms related to health data could be reconsidered.

3 Data Protection in General: Data Subject Responsible

Current laws and regulations on privacy and data protection heavily rely on the concept of informational self-determination (Cavoukian 2015)—the ability of individuals to have control over the collection, use, and disclosure of their personal information—on autonomous choice and consent (Austin 2014). This is what Solove (2013) refers to as "privacy self-management": rights that provide people with control over their own personal data. According to Solove, this control helps people to "decide for themselves how to weigh the costs and benefits of the collection, use and disclosure of their information". He argues that it would be paternalistic to protect people against their own bad decisions: "people make decisions all the time that are not in their best interest. People relinquish rights and take bad risks, and the law often does not stop them."

In this interpretation, the regulatory framework presumes a high degree of consumer knowledge, a freedom of choice and autonomous, "empowered" consumers. In practice, however, in particular online consumers are all but empowered individuals. Due to a lack of transparency in the market, and the absence of a true choice, consumers cannot take up responsibility for the protection of their own personal data (Zwitter 2014).

Consumers who want to make use of free online services and social media, like Google, Facebook, or the apps on their phones do not have real choice but to agree to the terms and conditions. This is not a matter of free choice, but of enforced choice (Carolan 2016). The current system is based on coercion, forcing consumers to accept all terms and conditions of search engines, websites, and social media just by clicking "OK" and to agree to the commercial use of their personal data. As the Minister of Economic Affairs of Cyprus phrased it at the conference in Nicosia November 2017: "The statement that someone has read terms and conditions is the biggest lie of the century."

Consumers, most of the time, are not really aware what personal data is being collected by companies, and are therefore not familiar with the data protection risks they run. Online reality outpaces "the idea that it is possible or desirable for every individual to monitor and manage a shifting collection of privacy settings of which they may only be dimly aware" (Richards and King 2014). Even if consumers read a privacy policy, it is almost never sufficiently clear for the person concerned that his personal data are used and for what purpose (Zuiderveen Borgesius 2014). How many LinkedIn users were aware of the possibility that their personal profiles were sold to third parties, and eventually to Microsoft? As Whittington and Hoofnagle (2012) remark: "Having spent time reading a privacy policy, the consumer may still not discover critical terms, such as whether the company sells personal information to third parties. Many privacy policies use vague, innocuous-sounding terms to mask third-party information sharing".

Consequently, consent in current data protection law has become "tainted" by unfair bargaining conditions and has lost its effectiveness altogether (Schermer et al. 2014). A lack of knowledge and information renders the classical privacy/consent based framework inadequate. Any form of self-determination on the decision whether one should share or sell his or her personal data has become illusory.

The objections with regard to the underlying principles of privacy law and data regulation are acknowledged by many, but satisfactory solutions are difficult to come up with. For example, Opinion 4/2015 of the EDPS,[2] does suggest a radically new approach towards the question of "the ever-increasing amounts of personal information being collected and processed in increasingly opaque and complex ways". However, it does not offer new solutions to get out of the deadlock. On the contrary, it presents the same, well-known framework that leans heavily on empowered individuals, accountable controllers, and innovative privacy engineering. Neither does the General Data Protection Regulation seem to address the

[2] Opinion EDPS, September 11th 2015, "Towards a new digital ethics. Data, dignity and technology".

inadequacies of the regulatory system nor bring any substantive changes in this situation, although consumers are granted the right to object to (profiling related to) direct marketing.[3] Law is still based predominantly on the misconception that consumers understand the rules of data collection, are well informed, and are digitally savvy enough to be able to realize an adequate level of data protection themselves. Giving up personal data to get some product or online service "for free" is considered as an inevitable consequence of taking part in the digital world of today.

Legal authors have struggled with the above-mentioned problems on current privacy and data protection laws. Some of them propose, for example, a more flexible regulation of data protection by introducing a less strict form of consent (Schermer et al. 2014). Others discuss a proprietary approach vesting a property right on personal data (Prins 2006; Purtova 2011), or a "privacy 2.0 approach", which leaves less room for the principle of purpose limitation;[4] or, rules of unfair trading practices could be an alternative for privacy regulation (Hartzog and Solove 2015).

However, the proposed solutions do not offer a truly satisfactory solution to the concerns the majority of consumers experience. We do not believe that these problems can be addressed simply by adjusting the conditions within which the data market operates. Even if the solutions proposed resulted in fair background conditions, well-informed consumers, a transparent market, explicit consent, even the possibility for consumers to vest property rights to their own data, the aversion, and moral concerns on the commodification and commercialization of personal data will not disappear. We encounter what lies beyond simple market-driven practices. This leads to the question whether there may be "some things that money should not buy?" (Sandel 2013).

Our conclusion is that privacy law and data protection rules alone do not offer enough protection to consumers who are concerned that their identities are fragmented into marketable parts and feel uneasy having to sell those parts whenever they are online. This unease can neither be explained by the single fact that people feel coerced to sell their data in exchange for (free) online services and consequently lose control over the process, nor can this be addressed by simply adjusting the market conditions, as liberal consent theorists believe. Other dimensions of life than privacy are at stake here, selling data per se can be more fundamentally, intrinsically degrading.

[3] 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). Art 21 (2): Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.

[4] Moerel and Prins (2015).

4 Body Parts and Data

We believe that looking into a different field of law, namely biotechnology law, and the role human dignity plays in this field may help us articulate new approaches to data protection. Human dignity is commonly approached from two perspectives. One is dignity as empowerment, as respect for autonomy. We use dignity here in another sense, viz. dignity as a constraint, as protection against instrumentalization.

It may seem infeasible to bridge the conceptual gap between the human body and personal information, but as already touched upon in the introduction this might be less far-fetched than it seems. Obviously, the legal status of human body parts does not correspond with the status of personal data entirely, but there are good grounds to make the comparison.

Current technologies have enabled medical science to isolate, process, change, and exploit parts of the body (like organs, blood, embryos, stem cells, and tissues) to be used for medical, scientific, and commercial purposes. Parts that previously were inextricably linked to the human body are now considered as a useful resource. This process of objectifying the individual has enabled the industry to extract, use, and market body parts without reference to the person involved. It is often observed that here practices are permeated by commercial metaphors. These metaphors in biotechnology reflect the reduction of the person into marketable body parts: "bodies are mined like a resource and organs are harvested like a crop" (Andrews and Nelkin 1998). This process shows resemblance with the harvesting of personal data in the context of big data applications, and considered by the companies as the "oil of the internet".

The developments in the domain of medical biotechnology have put pressure on the idea of the unity of the person and the body. Just like the development of Big Data practices and datafication have turned persons into (data-)objects, packages of data that are subsequently stripped and fragmented, analyzed and sold, bio technologies have deprived the human body of its organic unity and have transformed the human body into a kit of useful (exploitable) "bio-materials" (Van Beers 2017). Both biotechnology and in data processing and data analytic practices, parts of the person or identity of individuals are separated from the individuals themselves. Both practices render persons into an endless source of use values: bio products and personal data. In this sense, the legal status of personal data and human body parts can be compared; or, as Mittelstadt and Floridi (2016) noted, "it is likely more ethically problematic to strip context from data used to track the behaviors of individuals than it is to remove identifying information from tissue samples for medical research".

The ethical issues surrounding the human body have resulted in an extensive regulation of medical biotechnology provided with many legal prohibitions and restrictions. In (international) bio-regulatory instruments, the conception of *human dignity* plays a dominant (constraining) role where it prescribes the limits of modern

technologies (Beyleveld and Brownsword 2002). For instance, Article 1 of the Convention on Human Rights and Biomedicine of the Council of Europe:

> Parties to this Convention shall protect the dignity and identity of all human beings and guarantee everyone, without discrimination, respect for their integrity and other rights and fundamental freedoms with regard to the application of biology and medicine

Article 1 and 2(a) of the Universal Declaration on the Human Genome and Human Rights:

> The human genome underlies the fundamental unity of all members of the human family, as well as the recognition of their inherent dignity and diversity. In a symbolic sense, it is the heritage of humanity
>
> Everyone has a right to respect for their dignity and for their rights regardless of their genetic characteristics

Article 1 of the International Declaration on Human Genetic Data:

> The aims of this Declaration are: to ensure the respect of human dignity and protection of human rights and fundamental freedoms in the collection, processing, use and storage of human genetic data, human proteomic data and of the biological samples from which they are derived […]

Article 2(c) and 3(1) Universal Declaration on Bioethics and Human Rights:

> The aims of this Declaration are: to promote respect for human dignity and protect human rights, by ensuring respect for the life of human beings, and fundamental freedoms
>
> Human dignity, human rights and fundamental freedoms are to be fully respected.

One specific way in which the concept finds its expression in the regulation of biomedical technology is that human dignity in itself is contradictory with the commodification and the trade of human body parts: the principle of non-commercialization. The principle that the human body is *extra commercium* applies to all parts of the human body: i.e. tissue, blood, organs, eggs, sperm, and embryos. The prohibition of so-called transplant commercialism is found in numerous declarations and treaties,[5] where transplant commercialism is defined as "…a policy or practice in which an organ is treated as a commodity, including by being bought or sold or used for material gain".[6] The trade of human cells, tissues, and organs is prohibited as it is inconsistent with the most basic human values and would imply the instrumentalization of the personhood that contravenes the Universal Declaration of Human Rights.

Moreover, payment for human body parts is likely to take unfair advantage of vulnerable groups of people and leads to profiteering and human trafficking. The principle of non-commercialization conveys the idea that people lack dignity once

[5] See Convention on Human Rights and Biomedicine **Article 21 – Prohibition of financial gain:** The human body and its parts shall not, as such, give rise to financial gain. See *Istanbul Declaration on Organ Trafficking and Transplant Tourism 2008.*

[6] http://hottproject.com/about-the-crime/other-crimes/transplant-commercialism.html.

they are used by others as mere objects. This draws upon the writings of Kant (1797):

> A human being cannot be used merely as a means by any human being (…) but must always be used at the same time as an end. It is just in this that his dignity (personality) consists (…). [H]e cannot give himself away for any price (this would conflict with his duty of self-esteem) …

The principle of non-commercialization is reflected, for example, in the practice in the Netherlands (and in the United Kingdom) that blood donors are not paid, but only modestly reimbursed for their donation of blood (Petrini 2012). The principle that the human body should be neither commercialized nor a source of gain seems no subject of discussion: many countries at least in Europe have laws that embrace human dignity as constraint and prohibit the purchase or sale of body parts.

Dignity as constraint and the principle of non-commercialization have up until now been left out of the debate on data protection law. Instead, in privacy and data protection law, dignity as empowerment and the principles of individual autonomy and consent, as instruments of self-determination, prevail. It is however precisely the former, constraining dimension that could be of help in trying to find ways to offer better legal protection for digital consumers. Introducing the dimension of human dignity as a constraint enables us to reconsider the legal issues in the discussion on commercial use of personal data on the internet from a different angle (Brownsword 2007).

For the sake of this argument, an analogy must be drawn between parts of the human body on the one hand and personal data as parts of the personal identity of a human being on the other. The financial gain of the trade of body parts, whether for the person from whom these parts have been removed or for a third party, must be compared to the financial gain of data trade. Like in the bio-market, the prohibition of commercialization of data would apply to the individual whose personal data are purchased in exchange for free access to internet services and to the third parties: corporate entities of which the business models depend on the trade of human identities. The absence of any regulation where the parallel between body parts and data processing is drawn could be considered as a legal inconsistency.

5 Towards an Alternative Data Protection Approach

In this section, we elaborate on three alternative ways to approach data protection law, inspired by the law on biotechnology just discussed. Subsequently, we address health data and the concepts of paternalism and dignity.

5.1 Explicit Consent for Processing of Health Data

It is considered a crime to sell your organs, but what if health data are sold, and people agree to this transaction? Article 4(11) GDPR has a very strict definition of consent:

> 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

As already referred to above, Article 9(1) GDPR prohibits the processing of special categories of data such as:

> (…) the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health (…)

There are several exceptions to this ban on processing of special categories of data, relevant for now is the following one:

> 2. Paragraph 1 shall not apply if one of the following applies:
>
> (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject (…)

Whereas Article 4(11) presents a type of consent that seems the most rigid possible, here the GDPR uses the concept *explicit* consent. This is not the place to discuss what this addition "explicit" entails, but we have not encountered yet someone, who could come up with a meaningful distinction between consent in the sense of Article 4(11) and explicit consent. This was also the outcome of a discussion during the November 2017 REDA conference in Nicosia, Cyprus.

Health data may be provided by the data subject for free, but normally there is a reward, e.g. a service is provided in return. In case of organ trade, if someone provides his organs without monetary reward this is allowed, but if money is received in return this is considered a crime. The rationale is that trade is only possible when there are at least two parties (and often third parties, intermediaries), so also the one who provides the body parts falls under the scope of the regulation. Also, and in particular, intermediaries and the one who receives the organ are condemned. However, to stop transactions, criminalizing the donor is considered necessary. In the context of data protection the donor, viz. data subject, is not the one on which the normative framework should concentrate from an enforcement perspective. Rather, the parties collecting and processing the data are the ones relevant here.

5.2 Paternalism and Health Data

Paternalism is a recurring issue when regulation is aimed at protecting people (Moore 2013). In the context of organ trade, Conly (2012, p. 3) writes "We should save people from doing things that are gravely bad for them when they do that only as a result of an error in thinking (…) government should intervene in cases of obvious harm (…) I argue for paternalistic laws, and more specifically, paternalism of the sort that forces people to act, or refrain from acting, according to their best interests."

One reason for a paternalistic approach is that in case of the sale of organs, debate is that genuine and free consent is impossible. To what extent is free consent, in particular in the (explicit) GDPR sense, possible in case of data processing? The answer is that often it is not. In some of these cases, a paternalistic government approach should be considered (Allen 2015). One is the right to data portability in the context of health data. If citizens get control over health data, they can also provide these data to interested commercial parties. We doubt whether citizens realize the possible impact of having their health data analyzed by commercial parties. On consent and health data, there is also a flip side to this issue. Since consent should be freely given, and in case of health data explicitly, data protection law can also prevent rather innocent processing activities. One example is an outing with the company you are working with. Assume they want to climb walls, and some health data need to be provided to the company of the climbing wall. The employer cannot get consent for obtaining these data, since due to the power relation freely given consent is not possible. As we briefly sketched above, we should strive for data processing that covers all sides of the spectrum: no or fewer constraints in case of rather innocent data processing, and firmer constraints and maybe even a ban for intrusive data processing activities.

Is it a task for governments to protect, more than under the GDPR is the case, citizens against the processing of (health) data? There is a thin line between justified government interference and unduly paternalism. Privacy advocates are easy targets for accusations of paternalism: "If you really considered it, you would not give permission!", "Don't click okay blindly." Still privacy, and in the European Union even data protection, are fundamental rights (Van der Sloot 2017). Therefore, it could be considered the duty of government to protect its citizens in this respect and create further safeguards (Wisman 2019). But how, and to what extent?

A relevant angle for a refined approach to data processing is including ethical considerations. Roughly put, for legal and tech phenomena in general and data processing in particular, at least three questions are relevant. The first is about the technology, what is possible? The second is about the law, what is permissible? But even within the limits of the law, ethics should play a role, viz. what is desirable? To some extent this is covered by the Article 5(1) GDPR principle "fair processing". Processing should be fair, in relation to both a particular data subject and society at large. In relation to body parts, Kishore (2005) states "Arguments against organ sale are grounded in two broad considerations: (1) sale is contrary to human dignity, and

(2) sale violates equity (…) they reflect a state of moral paternalism rather than pragmatism." We claim that sometimes data processing can be non-ethical, against human dignity. An example is the commercial exploitation of health data of vulnerable people.

5.3 Dignity

In the GDPR, not much reference to dignity can be found, actually, only once, in the case of processing in the context of employment. Article 88(2) GDPR states "Those rules shall include suitable and specific measures to **safeguard the data subject's human dignity**, legitimate interests and fundamental rights…".

Post (2018) correctly observes that the GDPR is based on Article 8 EU Charter of fundamental rights, in which data protection is presented as a fundamental right. It is somewhat strange, amongst all those other fundamental rights, because the description is instrumental, even explicitly referring to fair information processing principles such as purpose specification, consent, and correction rights. This is different from the right to privacy in Article 7 of the EU Charter of fundamental rights:

> In contrast to data privacy, Article 7 of the Charter of Fundamental Rights of the European Union is entitled "Respect for Family and Private Life." (…) protects the dignity of persons by controlling inappropriate communications that threaten to degrade, humiliate or mortify them. (…) Article 7 enshrines the same privacy values as those safeguarded by the American tort of public disclosure of private facts. It protects what we may call "dignitary privacy."

These different approaches to data protection and privacy might explain why there is not room for dignity in the GDPR. It might be also the reason there is not a single reference to privacy in the GDPR (except twice in a footnote when reference is made to the ePrivacy directive). In earlier versions, privacy was mentioned. The rigorous "privacy cleaning" of the GPDR has also led to the renaming of the well-known concepts Privacy by Design, Privacy by Default, and Privacy Impact Assessment to Data protection by design, Data protection by default, and Data protection impact assessment. However, even from the perspective of data protection, as described in Article 8 of the Charter, the concept of dignity should not be left out of the picture totally. Article 1 of the Charter, after all, is about dignity, and as the Fundamental Rights Agency explains[7]: "It results that none of the rights laid down in this Charter may be used to harm the dignity of another person". Thus, there is even fundamental backing for looking at dignity in the context of data protection.

Hence, based on dignity, there are situations where individuals should be allowed to permit the collecting, gathering, and deriving of their personal data. We discussed Article 9(2)(a) and that the processing of health data could in some situations even be prohibited if the data subject gives explicit consent. The responsibility for respecting a prohibition based on dignity should not be placed at the realms of the

[7] http://fra.europa.eu/en/charterpedia/article/1-human-dignity.

individual or data subject, rather the focus has to be directed to the controllers and processors of personal data (De Hingh 2018).

6 Conclusion

Were it not for the law, parts of the human body like blood and skin could be an inexhaustible source of income—just like personal data are today. On a massive scale, large parts of our identity and our personality are commodified and becoming the object of trade. The fundamental right to privacy and data protection do not suffice to explain this discomfort or to tackle the legal issues arising from it. The commodification of our personal data as part of the online infrastructure of today does not affect the right to privacy alone but goes further by touching upon more fundamental conditions of being human, the deformation of which interferes deeply with the core of our human dignity.

Therefore, we propose to reorient the debate on data processing by introducing the notion of human dignity as constraint into the discussion. A prohibition of personal data commercialism (analogous to a prohibition of transplant commercialism) could contribute to a more future-proof regulation of data processing activities. Legal instruments similar to the ones concerning the human body could be applied to the trade of personal data as well.

Today, numerous (online) companies have developed business models based on the trade of personal data. However, none of the "potential benefits of the new technologies *really depend* on the collection and analysis of the personally identifiable information of billions of individuals".[8] The collection and processing of personal data is by definition neither indispensable when doing business on the internet, nor is data processing an absolute prerequisite for the functioning of online services. Against this background, there are no obstacles to limit or prohibit the use of this technology at least in areas where human dignity is evidently at stake, such as many situations where health data are being processed for commercial purposes.

References

Allen AL (2015) Unpopular privacy. What must we hide? Oxford University Press

Andrews L, Nelkin D (1998) Whose body is it anyway? Disputes over body tissue in a biotechnology age. The Lancet 351(9095):53–57

Austin LM (2014) Enough about me: why privacy is about power, not consent (or harm). In: Sarat A (ed) A world without privacy: what law can and should do? Cambridge University Press

Bamberger KA, Mulligan DK (2015) Privacy on the ground. Driving corporate behavior in the United States and Europe. The MIT Press

[8] Opinion EDPS, see note 2.

Beyleveld D, Brownsword R (2002) Human dignity in bioethics and biolaw. Oxford University Press
Brownsword R (2007) Rights, regulation, and the technological revolution. Oxford University Press
Bygrave LA (2018) Legal scholarship on data protection: future challenges and directions. In: Degrave E, de Terwangne C, Dusollier S, Queck R (eds) Law, norms and freedoms in cyberspace: Liber Amicorum Yves Poullet. Larcier, pp 493–504
Carolan E (2016) The continuing problems with online consent under the EU's emerging data protection principles. Comput Law Secur Rev 32(3):462–473
Cavoukian A (2015) Evolving FIPPs: proactive approaches to privacy, not privacy paternalism. In: Gutwirth S, Leenes R, de Hert P (eds) Reforming European Data Protection Law. Law, Governance and Technology Series, vol 20. Springer, Dordrecht
Conly S (2012) Against autonomy. Justifying coercive paternalism. Cambridge University Press
De Hingh A (2018) Some reflections on dignity as an alternative legal concept in data protection regulation. German Law J 19(05):1269–1290
Hartzog W, Solove DJ (2015) The scope and potential of FTC Data Protection. George Wash Law Rev 83:2230; GWU Law School Public Law Research Paper No. 2014-40; GWU Legal Studies Research Paper No. 2014-40. https://ssrn.com/abstract=2461096
Husak DN (2009) Legal paternalism. In: LaFollette H (ed) The Oxford handbook of practical ethics
Kant I (1797) The metaphysics of morals (trans: Gregor MJ). Cambridge University Press, 1991
Kishore HH (2005) Human organs, scarcities, and sale: morality revisited. J Med Ethics 31:362–365
Markou C (2011) Consumer-oriented software agents in the buying process: risks, issues and the EU legal response. Ph.D. thesis, University of Lancaster, Lancaster
Mittelstadt D, Floridi L (2016) The ethics of biomedical big data. Springer
Moerel L, Prins C (2015) On the death of purpose limitation. Privacy perspectives, 2 June 2015. http://Iiap.org/news/a/on-the-death-of-purpose-limitation
Moore AD (2013) Coercing privacy and moderate paternalism: Allen on unpopular privacy (February 26, 2013). https://ssrn.com/abstract=2225376
Newell S, Marabelli M (2015) Strategic opportunities (and challenges) of algorithmic decision-making: a call for action on the long-term societal effects of 'datification'. J Strateg Info Syst 24(1):3–14
OECD (2013) Exploring the economics of data: a survey of methodologies for measuring monetary value. OECD digital economy papers, no 220. OECD Publishing
Petrini C (2012) Ethical and legal considerations regarding the ownership and commercial use of human biological materials and their derivatives. J Blood Med 3:87–96
Post R (2018) Data privacy and dignitary privacy: Google Spain, the right to be forgotten, and the construction of the public sphere. Duke Law J 67(5)
Prins C (2006) Property and privacy: European perspectives and the commodification of our identity. In: Guibault L, Hugenholtz PB (eds) The future of the public domain. Kluwer Law International, Deventer, pp 223–257
Purtova NN (2011) Property rights in personal data: a European perspective. BOXPress BV, Oisterwijk
Richards NM, King J (2014) Big data ethics. Wake Forest Law Rev 49:393–432
Sandel MJ (2013) What money can't buy: the moral limits of markets. Farrar, Straus and Giroux; Reprint edition (April 2, 2013)
Schermer BW, Custers B, van der Hof S (2014) The crisis of consent: how stronger legal protection may lead to weaker consent in data protection. Ethics Info Technol 16(2):171–182
Schwartz PM (2004) Property, privacy, and personal data. Harv Law Rev 117(7):2056–2128
Smutny Z, Janoscik V, Cermak R (2017) Generation Y and internet privacy: implication for commercialization of social networking services. In: Benson V, Saridakis G, Tuninga R (eds) Analyzing the strategic role of social networking in firm growth and productivity. IGI Global, Hershey, pp 95–119

Solove DJ (2013) Privacy self-management and the consent dilemma. Harv Law Rev 126:1880
Van Beers BC (2017) Imagining future people in biomedical law: from technological utopias to legal dystopias within the regulation of human genetic modification technologies. In: Ambrus M, Rayfuse R, Werner W (eds) Risk and the regulation of uncertainty in international law. Oxford University Press, Oxford, pp 117–140
Van der Sloot B (2017) Legal fundamentalism: is data protection really a fundamental right? In: Leenes R, van Brakel R, Gutwirth S, De Hert P (eds) Data protection and privacy: (in)visibilities and infrastructures. Springer, pp 3–30
Whittington J, Hoofnagle CJ (2012) Unpacking privacy's price. N C Law Rev 90:1327
Wisman THA (2019) The quest for the effective protection of the right to privacy: on the policy and rulemaking concerning mandatory Internet of Things systems in the European Union. Ph.D. thesis, Vrije Universiteit Amsterdam
Zuiderveen Borgesius FJ (2014) Improving privacy protection in the area of behavioural targeting. Ph.D. thesis, UvA Amsterdam
Zwitter A (2014) Big data ethics. Big Data Soc: 1–6