Informational Self-Determination, Digital Health and New Features of Data Protection

Theo Hooghiemstra*

Health data outside the medical context should be better protected against governments and companies. The advance of personalised health environments changes the meaning of informational self-determination in healthcare. Outside the medical context, there is an imbalance between people’s ability to truly determine the usage of their health data and the data power of companies and governments. To create a proper balance, people need additional protection, for which I propose a coherent set of recommendations in my dissertation: patient confidentiality by law, prohibition of the trade in health data, a digital butler and the rest of the recommendations I mentioned.

Keywords: Informational Self-Determination, Digital Health, Digital Butler

I. Introduction

In the 1970s and 80s, the term ‘informational self-determination’ first emerged in Germany.

Whilst it is mostly defensive in nature, the message to the government is clear: leave me alone! However, it is to be noted that informational self-determination can also be offensive when considering a right of access, right to deletion etc. Today, smartphones and the Internet in particular are conveying a strong message to all parties: let me manage my own data! The term ‘onlife’ is therefore appropriate especially when considering digital health and the General Data Protection Regulation (GDPR) that has now succumbed to being ‘the law of everything’1. The broad definition adopted with regards to ‘personal data’ has not only shifted the future of EU data protection law but has also altered the nature of control one has over their own personal data2. This transition from negative to positive freedom inspired several questions I will aim to answers in this article3. For example: How do existing regulations compare to these trends? And are there any facts or standards which can be used as a predictor? On the basis of several preceding works of legal philosophers, the present article argues that the following four standards should be met by any regulation:

1. Human dignity: we cannot put a price on the value of man.
2. Receptiveness to changes in society.
3. Regard for the context. Within my research, this would be the context of health data that have ended up outside the medical context.
4. Legal protection.

In this article I present the content of my dissertation on informational self-determination and digital health by outlining:

a) the topic that is to be investigated;

b) the theoretical and legal background;

c) discussion of the new features of data protection and the practical examples;

d) conclusions and recommendations.

II. The Topic

Within my dissertation, information self-determination is defined as ‘the ability of a person to...

DOI: 10.21552/edpl/2019/2/6

* Dr Theo Hooghiemstra obtained his PhD from the University of Tilburg on Informational self-determination in healthcare and is one of the founders of Hooghiemstra & Partners. For correspondence: <theo@hooghiemstra-en-partners.nl>.


2 ibid.

determine, in principle, the extent to which their personal data are used and further disclosed, with a view to achieving a self-determined life. The degree to which individuals actually have the ability to determine the extent personal health-related data about them are used has been significantly influenced by the rise of personalised health environments available through mobile data carriers. That being said, there is no merit in being for or against personalised health environments as they already exist (inter)nationally.

According to MedMij\(^4\), one of the leading health environments regulators in the Netherlands, a personal health environment is defined as follows:

A personal health environment is a digital environment that enables the user to access all of their relevant health data, which is stored across several healthcare professionals, healthcare providers and governments, to supplement it with self-generated data and to share it with whomever they want. Personalised health environments provide access to all of the individual’s health data through websites and apps.

This article has four research questions:

1. What should be understood by informational self-determination in light of technological developments? Is informational self-determination possible and desirable? If yes, to what extent and with what limitations, and whether a distinction should be made between types of persons?

2. What does this mean in concrete terms for the field of health and healthcare?

3. What does this mean in concrete terms for the field of health and healthcare?

4. Given the rise of personalised digital health environments, what other forward-looking recommendations and methods can be made to achieve informational self-determination?

III. Theoretical and Legal Background

1. Introduction to the Theoretical and Legal Background

As is the case with most technological innovations, the new playing field of personalised digital health environments offers opportunities but also entail of many risks. While some people will view the new possibilities as attractive and useful, the wider availability of health data also raises fundamental questions which challenge the traditional normative mechanism of medical secrecy.

Health data has long been qualified as ‘special’ or ‘sensitive’ data and thus deserves extra care and protection\(^5\). Before modern regulation of privacy and data protection, medical confidentiality was practiced with a pledge of secrecy and the right to refuse to give evidence. Both of these constraints were strictly interpreted by medical professionals and courts\(^6\). Since then, medical confidentiality, the pledge of secrecy and the right to refuse medical evidence have been put under pressure – partly due to social and technological developments. When individuals manage their own health data, the traditional protective approach of medical confidentiality is largely lost. Even if encrypted on personal devices, the risk of misuse still remains great as encryption does not necessarily guarantee the proper use of this ‘sensitive’ data. However, it can also be said that public and private organisations also have the capacity to mishandle data. These new developments require more thought in order to ensure that an essential function of law, namely the orderly and proper streamlining of social, economic and technological change, is maintained. This holds especially true in light of recent technological developments.

Since we are dealing with legal protection in the broad sense, I would like to touch upon the work of the legal sociologists Nonet and Selznick titled *Law and Society in Transition: Towards Responsive Law*.

---


\(^6\) HR 19 November 1985, NJ 1986, 533, annotatie van’t Hart (Verschoningsrecht).
Nonet and Selzick distinguish the following three ideal types of law:
1. Repressive law: the law as an instrument of the political elite.
2. Autonomous law: the right as a counterpart of politics, in which abuse of power is countered by means of legal protection in the form of rules and procedures.
3. Responsive law: with the aim of increasing social justice.

Nonet and Selzick argue that these three ideal types of consecutive phases of law form an evolution. In their view, responsive law is the most advanced because in a system of responsive law legality is not enough. Justice in this system is considered the yardstick of the rule of law. Their argument in favour of responsive law does not mean that legal protection through autonomous and repressive law should be removed but should nonetheless be considered essential to the whole. As such, legal protection manifests itself in two ways; either through prevention by anticipating possible problems in current and future developments or through autonomy and repressive legal protection. Responsive law and repressive legal protection mean that during both the design and the implementation phase of law in the real world the protection of persons must be taken into account. This implies that designers have an obligation to achieve results which will anticipate potential problems. These must be quick and user-friendly ways to address any practical issue. In the context of medical care and the GDPR, practical issues may arise around consent. This is especially important when it involves the ethical and legal questions about things being done to our bodies.

In addition to responsive law, autonomous and repressive power against the dominating position of companies and governments remains necessary. Strong regulators and a digitally competent judiciary must act on the basis of robust legislation against mala fide companies or governments that abuse the dependent position which people find themselves in. In concrete terms, this can be seen in the various manifestations of the phenomenon of cybercrime. For example, the global attack Wannacry in May 2017 particularly affected hospitals in the United Kingdom. The illicit trade on the Darkweb has seen a rise in medical information which is worth significantly more than credit card information.

2. Theoretical Background

I was inspired theoretically, legally and morally by Fuller’s principles of legality (ie his eight rules for genuine laws) and the social theory of the legal sociologist and philosopher Selzick. Finally, Berlin’s ‘Two Concepts of Liberty’ (ie negative and positive liberty) and Nissenbaum’s contextual approach to informational self-determination and privacy are two important writers for the present article. On the basis of the ideas of these legal philosophers a normative model consisting of the following four parts was formed:

a) human dignity;
b) responsive regulation;
c) contextual integrity;
d) legal protection.

a. Human Dignity

A comparative legal study on the right of access to information in Sweden, Germany, France, Belgium, the United States of America and Canada showed that the right to informational self-determination was first recognised by the German Constitutional Court in 1983. This right was based on the inviolability of human dignity and the right of everyone to freely develop their personality. The protection of human dignity is therefore the guiding principle in the first question to be examined within the normative framework. Informational self-determination in healthcare is, therefore, to a large extent, based not only on the inequality of knowledge but also on the inequality of power in the doctor/patient relationship. It is evident that doctors and other healthcare workers have a special trust relationship where it is crucial to avoid improper use of personal data.

Human dignity can thus be considered a fundamental value when it comes to ensuring self-determination. It is a concept used in many philosophical

---

7 Suzan Verbeek, Probleemoplossend strafrecht en het ideaal van responsieve rechtspraak (Sdu Uitgevers 2011).
9 Also called deepweb, a part of the global web that cannot be found directly by regular search engines, but only through special software and passwords. In addition to journalists, whistle blowers and cryptocurrencies, criminal and terrorist organisations also use it to carry out illegal transactions that are difficult to trace.
and religious traditions. Since the Enlightenment, Kant’s definition of human dignity can be considered authoritative. However, according to Kant, only man meets this definition, and therefore has absolute value and is an objective to be met in itself. I would link this to the paragraph below and not have a separate paragraph as the latter explains what ‘definition is to be met’. The principle of human dignity, underpins human rights, especially within the framework of the Council of Europe. A comprehensive legal study conducted by Van Beers on the comparison between how different legal systems incorporate the concept of human dignity has found that the power of disposal is a bi-product of biomedical technology. The latter is however restricted. According to Van Beers, it is this principle that ultimately forms the basis for protection against the risks of instrumentalisation, commercialisation and ultimately the dehumanisation of human beings.

This basis is not only relevant for biomedical technology, but also for informational self-determination. Van Beers conducted an analysis of the case law of the European Court of Human Rights (ECtHR) and an extensive consideration of well-known European Convention on Human Rights (ECHR) case law with regard to assisted suicide\(^{10}\), transsexuality\(^{11}\), sexual freedom. He concluded that, although human dignity is the starting point for the ECtHR\(^{12}\) as seen through the case law above, Article 8 of the ECHR\(^{13}\) has indirectly recognised a right to physical self-determination. This is also expressed in the Universal Declaration of Human Rights (UDHR) whereby rights are derived through human dignity.

From the perspective of human dignity, self-determination has great importance. In particular, self-determination as freedom of choice and as self-fulfilment are essential within this context. However, human dignity has an even broader and deeper meaning because it also protects those who do not have complete self-determination, for example, vulnerable or disabled people. As seen above, the right to self-determination can be derived from international human rights treaties and has now also been recognised in the case law of the ECtHR.\(^{14}\) The recognition of such a right, as well as the codification of human dignity, has been criticised by Rouvroy and Poulet. They do so on the basis that certain values, eg human dignity, autonomy and self-determination, should underpin human rights and that these values should be realised in the real world.\(^ {15}\) However, the values themselves do not need to be codified. Nevertheless, one can assume a right to self-determination that can be extended to ‘informational self-determination’.

b. Responsive Regulation

Fuller advocates for responsive governance, and like Selznick, develops the ideal that ‘legislators should take the perspective of those who have to work and live with the rules’.\(^ {16}\) For the development of my theoretical framework, the ideal of responsive regulation is relevant. Namely, because I bring together the ideal of responsive regulation with the conviction that people in the current information technology era should have the guarantee that informational self-determination actually represents something. In the digital world, traditional legal protection is not sufficient. The government has to play a much more active role to protect its citizens than in the past and should embrace that role much more.\(^ {17}\)

Selznick prioritises the maintenance and respect of the rule of law. At the same time, he has become known as a prominent advocate of responsive law. Selznick sees responsive law as the most advanced form of law – one which is reflexive to the changes in society. In addition to his own social theory, Selznick developed a theory together with Nonet. At its core, the theory of Nonet and Selznick consists of a typology of three ideal types in the form of a development model. Ideal types make it possible to provide insight into certain developments and structures, including underlying norms, values and motives.\(^ {18}\) The theoretical model will be applied as intended by Nonet and Selznick, namely, as an analyt-

---

10 Koch v Germany App no 497/09 (ECtHR, 19 July 2012).
11 B v France App no 13343/87 (ECtHR, 1992).
12 ECHR 1950, art 1.
13 Right to respect for private life.
14 Jysiac v Poland App no 541003 (ECtHR, 20 March 2007).
16 Willem Witteveen, De wet als kunstwerk, een andere filosofie van het recht (2nd edn, Boom Juridische uitgevers 2015).
18 Arne Zuurmond, De Informatie: een theoretische en empirische herorientatie op Weber’s idealtypen in het informatietijdperk (Phaedrus 1994) 27.
ical instrument. The theory focuses mostly on the search for 'the spirit' of the law.\textsuperscript{19}

The responsive ‘spirit’ is aimed at solving problems and realising social effects. The view that a correct application of the rules alone is not sufficient is also a central starting point of responsive law. Nonet and Selznick present, in a greater and more rudimentary manner, a development model of the law. Repressive law is inherently unstable because order and authority are not based on consent but is rather enforced. Authority is here exercised through digital oppression. Whether those who are subject to the rules agree to this is of secondary importance. As a result, the regime of repressive law lacks legitimacy. In a system of autonomous law, the rule of law applies. A great deal of importance is attached to adhering to rules and procedures. There is a risk, however, that although the law is properly applied, outcomes won’t be considered fair. In a system of responsive justice, lawfulness is not sufficient, but rather justice is the yardstick by which the legitimacy of the law is measured. Thus, responsive law is both a logical end point in the development of the law and an ideal. Yet, responsive law is also unstable because there is a dynamic dividing line between politics and law. As a result, responsive justice runs the risk of degenerating into a repressive justice system. In the following, I will address the question of where the limits of the use of responsive law lie. After all, there is a risk that regulation will become too flexible and possibly even arbitrary. This is the case of the GDPR, which has been criticised for its broadness.

c. Contextual Integrity

Medical confidentiality means that, in principle, individual healthcare providers may not disclose information about their patients to third parties. In other words, medical professionals have a duty of confidentiality towards their patients with regards to third parties.

Nouwt already wrote about the increasing pressures placed on medical confidentiality within healthcare due to the rise of the informational society in his 1997 dissertation.\textsuperscript{20} As such, health data are increasingly being processed outside the medical context of healthcare providers and patients. It is no longer about patients, but rather people and their daily lives. Therefore, ‘patient secrecy’\textsuperscript{21} seems advisable as legal protection for health data that is outside the scope of medical confidentiality. For example, in addition to the need of individual consent to enable controllers of a personalised health environment to process data, the law in the Netherlands also establishes a duty of confidentiality and a right to refuse to give evidence, which is comparable to medical confidentiality and acts as a safeguard\textsuperscript{22} for patient data that is no longer protected by medical confidentiality. In addition to ‘patient confidentiality’, the health data of people who have chosen to place their health data in a personalised health environment are ‘automatically’ protected. As a result, law enforcement agencies cannot infringe on the right of the doctor and other medical professionals to refuse to give evidence, simply because the patient has chosen to have his data available in personalised health environment applications and websites.

Nissenbaum’s theory of contextual integrity is one of the most influential ideas on privacy and informational self-determination of the past ten years. In this theory, Nissenbaum states that informational determination can be experienced as threatening to our privacy whilst at the same time protecting one’s privacy. For example, when visiting a general practitioner (GP), as a patient you expect the doctor to treat your personal information confidentially, but also to share it with specialists when necessary. These are standards that belong to this context. Therefore, if you find out that your doctor sold your data to a marketing company, you will conclude that information flow to be inappropriate and experience the GP’s behaviour as a gross violation of privacy. In other words, the norm has been violated and the integrity of the context of visiting GPs has been tarnished.

\textsuperscript{20} Sjaak Nouwt, ‘Zorg voor Privacy’ (PhD thesis, Tilburg University, 1997)
Nissenbaum takes historically grown and proven contexts as a starting point. The privacy standards are the same in the online world as in the offline world. Nissenbaum illustrates this by comparing the search for information in a library with a Google search. And despite the Google search being different from consulting a library catalogue, there are also similarities. Namely, both are done with the objective of research, the acquisition of knowledge and intellectual enrichment. It is precisely these activities that are important in liberal democracies. They should not be hindered by people looking over your shoulder or intrusive authorities.23

It is through this manner that Nissenbaum develops her 'contextual' approach. This contextual approach fits nicely with the theme of 'informational self-determination' in healthcare. After all, the healthcare context has always been a relational context. A key question is whether the core elements of this context should be able to be honoured or remain honoured if persons have their health data managed by parties, such as providers of personalised health data (applications, websites etc), which do not have medical treatment agreements. However, it can be questioned whether this is the case for personalised health environments. Nissenbaum sees the challenges in the fact that the Internet is changing the way information is collected, analysed and disseminated, and can therefore threaten the contextual integrity of our social lives. She points out that some companies have more power than States. As far as governments are concerned, the principles of good governance and constitutional law are important to keep oppressive forces under control, but can they withstand new developments? Do individuals with personalised health environments really have self-determination and insight into their health data? Or will this power mainly come into the hands of companies and governments? In the context of care, will there indeed be this suggested unlimited dynamic? Hospitals, healthcare institutions and GP practices will probably continue to manage data. For certain types of persons, those with chronic illnesses for example, ‘shared management’ is possible and useful. In this case, the question arises as to how the personal data should be protected.

The literature shows that the idea of shared decision-making is a fruitful starting point for the patient/healthcare provider relationship. Here, the patient is taken seriously and involved in the process24 For new developments outside the care context, such as personalised health environments and big data, additional precautions are necessary to protect individuals.

d. Legal Protection

Legal protection in the light of informational self-determination is about people being in a position where they can access their information as much as possible. This requires enforcement with transparent and effective supervision with the possibility of simple and accessible dispute resolution.

Besides inspiring ‘responsive’ regulation, we saw that Selznick is also influential regarding the normative question of whether there is an accessible and user-friendly form of legal protection and complaint handling mechanisms. Selznick’s social theory is still relevant in an analysis of current developments in technology and society as it connects the liberal ideal of self-determination with the need for institutional design. An institutional design to protect individuals and give as much self-determination as possible is in practice essential. At present, there are no specific institutional designs for personalised health environments.

In a philosophical sense, Selznick builds on Dewey’s American pragmatism. Within this article, I take Selznick’s fruitful moral perspective as a starting point for self-determination in today’s digital information society. Through analogy with Selznick’s position in the debate between idealists and realists, it is important to note that idealists tend to view technological change positively whilst realists tend to focus more on the dark side of the informational society we live in (ie cybercrime, data leaks, loss of privacy etc).

In his paper, ‘The Moral Commonwealth’, Selznick systematically links philosophical traditions with social theory. Selznick’s social theory is broad as it draws insights from sociology, psychology and organisational theory. In the liberalism/communitarianism debate, Selznick describes a form of liberal-com-

23 Helen Nissenbaum, Privacy in context: technology, policy, and integrity of social life (Stanford University Press 2011).
munitarianism in which the liberal ideal of freedom is linked to the ethics of social responsibility. His criticism of Dewey’s pragmatism is that it often has a too optimistic view of people and society and for obvious reasons, this is a difficult lesson for liberals and pragmatists.

Just like Hobbes, but unlike Dewey, Selznick points to the dark side of people. Only counterpower can control power, and that possibility must exist in every moral community, which is why procedures and structures are important. Translated into today’s digital informational society, protection and supervision are necessary to safeguard the self-determination of personal data, both against the power of governments and against the power of large data processing companies. Selznick’s responsive right is open to changes in society. In contrast, the GDPR is ill-suited for the rapidly changing information technology. Legal protection and complaint-handling mechanisms are not yet well regulated around personalised health environments with regard to social and technological developments. In the development of the predominantly private appointment system for personalised health environments and any future legislation for it, easy-to-access legal protection and complaint-handling mechanisms should be regulated.

A central question for governments is how they, as regulators, should respond to both the challenges and opportunities of a technology-driven society, without compromising or impeding on people’s ability to make choices with regards to their personal data. The legitimacy and effectiveness of this system is therefore based on conditions that must be respected in order to prevent some of the abuse outlined above. For example, in the ideal world of informational self-determination, individuals are obliged to manage their own data for economic reasons. This is often the case in the consumer world of traveling. The later demonstrates that whilst this is an attractive idea, as an ideology it can lead to abuse. As such, what measures should be taken to prevent this potential abuse?

This question can be answered through the works of Berlin who in his essay “Two Concepts of Liberty” made an interesting distinction between positive and negative liberty. Negative liberty is a restriction of one’s own domain, in which the State and others may not interfere: ‘freedom from’. In other words, it is about a right to defend oneself, about self-determination over one’s own private life. Although, whilst Berlin admits that this option is limited in scope, he considers it conceptually clear and therefore useful in a political and moral discussion.

Positive liberty is about ‘freedom to’ ie the availability of opportunities to ‘author’ your life and make it meaningful. Positive liberty requires stimulation by others to actually make self-determination possible. Berlin warns that a concept like positive liberty can evoke the danger of ideological abuse and political manipulation. Under the veil of a so-called ‘caring’ government or health insurer, there is a tendency to quickly transform ‘may’ into ‘must’, to transform a right into a duty - this is still relevant today in the world of personalised health environments and in the big data society we are living in.

We can therefore ask ourselves how to best prevent abuse in personalised health environments and how these complaints should be handled with regards to individuals who have had their data mismanaged for example. Government is increasingly applying a top down approach in its management of society. In the current system, the assumption is that enforcement will primarily have to be carried out by individuals themselves on the basis that they have been informed and have rights. Thus, the enforcement task lies primarily with individuals, and wrongly so. Following on from Nissenbaum, the enforcement task should primarily be placed with those responsible, for example, by obliging them to organise their processing on the basis of privacy by design. In addition to easy access, legal protection and privacy by design, counter-power to data-hungry companies and governments at a higher level is also necessary. A stronger judiciary and a regulator that acts on the basis of solid legislation and regulations are very much needed.

3. Legal Background

At the European level, the concept of informational self-determination is not as explicitly used as in Germany. The ECHR and the Court of Justice of the EU

25 Berlin (n 3).
(CJEU) do not explicitly include the right to informational self-determination. It is considered more of an implicit right to informational self-determination that can be inferred from the case law of the ECHR.  

In the early 1970s, the Council of Europe noted that Article 8 ECHR had a number of shortcomings in the light of technological and societal developments. This is particularly true from the perspective of the growing usage associated with technologies. However, with the increase of usage, there are many shortcomings including the uncertainty about the scope of ‘private life’, an emphasis on protection against infringements by ‘public authorities’, and the lack of a more proactive approach including possible misuse of personal data by companies and other relevant private sector organisations. This conclusion ultimately leads to the Data Protection Convention or Strasbourg Convention, resulting in a treaty to protect all individuals in Europe whilst at the same time respecting their fundamental rights and freedoms with regards to the automatic processing of personal data. Within this convention, personal data is defined as ‘any information relating to an identified or identifiable person’.  

The ‘protection of personal data’ in this treaty is broader than ‘privacy’ because it also covers all other rights and freedoms and all types of data (including ‘ordinary’ personal data and personal data in the private domain) regardless of their relationship with privacy. At the same time, ‘protection of personal data’ is also a more limited concept than privacy because it relates to the processing of personal data and not to other aspects of privacy such as spatial and relational privacy. The similarities and differences between the right to privacy - more precisely the ‘right to a private life’ - and the right to the protection of personal data are important, according to various authors. Privacy and the protection of personal data are both expressions of a universal idea with ethical dimensions: autonomy and human dignity.

There are, however, crucial differences between the two concepts. The notion of ‘protection of personal data’ was developed to provide structural, legal protection for individuals against the careless use of technology in the processing of personal data, regardless of whether it fits within the scope of respecting private life. The protection of personal data is a set of safeguards - essentially a system of checks and balances consisting of conditions, individual rights and independent supervision - for all personal data, sensitive or insensitive to private life. Data protection gives positive protection to all forms and types of data. According to Rodota, the developments in the concept of privacy have progressed from a right to be left alone to the right to have control over one’s own information to better determine what that person would like to keep ‘private’.

From a European perspective, the Strasbourg Convention, the OECD guidelines, the Charter and the GDPR are relevant. Nonetheless, I shall confine myself to the GDPR. The GDPR replaced the European Directive 95/46/EC on 25 May 2018. Its material scope does not differ much from the Directive and like the Directive, it deals with the protection of personal data and is also applicable in both the private and the public sector. The direct effect of the Regulation does not only provide greater consistency but also an increased territorial scope. The GDPR is a regulation, which is of general application, binding in its entirety and directly applicable in all EU Member States. Unlike the Directive, the GDPR makes its applicability very clear - it applies to the processing of personal data by controllers and processors in the European Union, regardless of whether the processing takes place in the EU. The GDPR also applies to the processing of personal data of data subjects in the European Union by a controller or processor not established in the EU, where the activities relate to: of-
ferring goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behaviour that takes place within the European Union. Kuner considers this the ‘Copernican revolution’ which refers to the shift of greater obligations and key responsibilities towards controllers and processors.

An important innovation of the GDPR is the placing of more responsibilities and obligations on the data controller, including the right of access\(^39\), right to rectification\(^40\), right to data portability\(^41\) etc. As previously mentioned, the amendment of the territorial scope is of great importance when considering the market of personalised health environments, with regards to the use of applications on smartphones, even if these services are located outside the EU. The GDPR does not only provide EU residents the right to receive personal data concerning him/her, which he/she has provided to the controller\(^42\) but the data subject has the right to object ‘at any time’\(^43\) to the processing of their personal data based on ‘compelling legitimate’\(^44\) grounds. Unlawful processing can therefore be challenged under civil or administrative law. However, in order to do so, individuals must know that an organisation processes personal data about them in the first place.

As a general rule, the GDPR prohibits the processing of special categories of personal data\(^45\). The category of special personal data also includes health data, as well as genetic data and biometric data. In addition, it is also generally prohibited to process personal data about a person’s religion or beliefs, race, political affiliation, sexual life and trade union membership. Biometric data as well is included in the GDPR as a category of special personal data insofar as they are processed in a manner in which the unique identification of a person is no longer traceable. Biometric data include fingerprints, voice, handwriting, hand contour geometry and scans of the retina, iris and face. The sensitivity of this data stems from the fact that they contain unique body characteristics of a person. The GDPR lists a number of exemptions to this general prohibition on processing special personal data. The exemptions to the ban on processing health data can be found in Article 9(2) of the GDPR. If the above-mentioned exemptions in the GDPR cannot be invoked to process health data, a data processor/controller may still be permitted to do so, if the person explicitly consents to this.\(^46\)

With explicit consent, it is permitted to process special personal data, eg health data. Unlike ‘unambiguous consent’, explicit consent requires that the person concerned has explicitly expressed his or her will; the data subject must have expressed his will to grant permission for the data processing verbally, in writing or through their behaviour. The controller has a double burden of proof to assume that someone has given his explicit consent. For example, if in doubt, it must be possible to prove that the particular consent has been given and for a specific purpose. Moreover, if necessary, it must be possible to demonstrate that the consent meets the requirements set. The responsible party will therefore have to be able to demonstrate that it has done everything that could have reasonably been expected of them, for example with regard to the provision of information to the data subject. The consent is not valid if it does not meet these requirements.

Anyone who processes personal data in general should be able to do so on at least one of the criteria found in Article 6 GDPR - this also applies to health data. A possible basis could be that the collection, recording and further use of personal health data is necessary for the execution of a medical treatment\(^47\) or results from the legal obligation to keep records. Further, the ‘unambiguous consent’ of the person involved\(^48\) is a possible basis for the collection and recording of personal data. However, where other bases may be used, the consent of the data subject is not necessary. The GDPR of course has even more provisions that apply to the processing of health data. In line with other laws, it stipulates that personal data may only be processed in a proper and careful manner.\(^49\)

Within the GDPR there are general obligations for a controller to take appropriate technical and organ-

---

39 GDPR, art 15.  
40 GDPR, art 16.  
41 GDPR, art 20.  
42 ibid.  
43 GDPR, art 21.  
44 ibid.  
45 GDPR, arts 8 and 10.  
46 GDPR, art 9(2).  
47 GDPR, art 6(1)(b).  
48 GDPR, art 6(a).  
49 GDPR, art 5(1)(a).
isational measures to protect personal data against loss or any other form of unlawful processing, such as unlawful access to health data. This obligation also includes the data minimisation principle that no excessive data should be processed than is necessary to the task at hand. This obligation is therefore also an incentive for data protection-by-design, which will be further elaborated in the next section. Information rights are thus considered a cornerstone within the GDPR. The assumption is that a person can actually exercise their right, because they know that information about them is being processed and by whom. This is partly based on the idea that it contributes to a person’s informational self-determination and offers them more control over data processing.

In the GDPR, a number of separate ‘informational self-determination rights’ have been expanded. Examples include the right to electronic access and the right to data portability. For personalised health environments, the right to data portability in Article 20 GDPR ‘only’ applies insofar as the person concerned has provided data in a medical file or personalised health environment, to the healthcare provider or to the supplier of a personalised health environment. In the case of a right to data portability for all data in a medical record or personalised health environment of the data subject, the development of personalised health environments would contribute even more to informational self-determination. We have yet to see how the new right will play out in the real world. However, should this new right – by limiting data to solely that provided by the individual – significantly hinder the practical development of informational self-determination through personalised health environments, legislation could be considered to broaden the scope of Article 20 GDPR.

Rouvroy and Poullet criticise the wording of the second paragraph of Article 8 ECHR on the protection of personal data, which suggests that consent is a sufficiently legitimate ground for data processing. The CJEU has issued several rulings on the protection of personal data. The most far-reaching and topical case is the influence of the Schrems case against Facebook which led to the termination of the Safe Harbour Agreement.

IV. New Features and Practical Examples

1. Introduction

Due to the turbulence of technological and social innovation, the law is in danger of lagging behind, which raises the question: How can we construct legal protection for those affected in a responsible manner?

This article will aim to provide a clear normative examination and explanation of legal mechanisms and at time remedies which may be used when looking specifically at personalised digital health environments. As it is impossible to provide a complete overview, I will focus on the key areas within this subject. With these considerations in mind, this section of my article will focus on the following research questions:

- Research question 1: Standardisation can take shape in the applications themselves, namely via data protection-by-design. Data protection-by-design and other possibilities have the potential to support individuals in managing their health data. However, what does this mean in concrete terms for the healthcare sector?
- Research question 2: Given the rise of personalised digital health environments, what other forward-looking recommendations are needed in order to provide informational self-determination?

Due to the fact that technological innovations are developing at a rapid pace, one should aim to embed legal protection at the technical stage as much as possible when drafting it. For example, taking the first research question into account, at the technical level it will be of necessity to work with the privacy-by-design model or, more broadly formulated, legal protection by design.

When it comes to the principle of human dignity, we are mainly dealing with issues of legislation and regulation. Such issues would concern, for example, supplementary provisions of law ensuring the data controllers’ right to refuse to give evidence regarding medical patients or the question of under which con-

50 GDPR, art 32.
51 GDPR, art 20.
ditions suppliers are allowed to offer personalised digital health environments. Perquisites could be specifically designed to prevent abuse. In terms of responsive regulation, we are mainly concerned with ensuring that rules are understandable and applicable. In other words, the laws should be manageable and workable for the layman. However, when it comes to contextual integrity, we are questioning whether the healthcare applications sufficiently consider the situation of people having to use them and people wishing to use these applications. Therefore, the main legal and technical obligations need to be more specific in order to better uphold the principle of human dignity.

This observation makes the following question relevant: what role can be expected from the government and therefore from the legislator?

In legal theory sense there is an argument to be made that minimal liberal legalism within few government interventions offers too little protection for individuals, especially where protection is urgently needed. At the same time, Berlin warned that a concept of positive liberty with an active government that imposes far-reaching obligations could evoke the risk of ideological abuse and political manipulation. Any risks must be eliminated technologically, organisationally or legally as much as possible. Translated into practical terms this means that those who may decide to make use of the possibilities of digital health environments should be able to rely on the fact that the applications comply with privacy-by-design, and the government and legislator should anticipate such developments by means of policy.

The search for meaningful informational self-determination in healthcare leads to the description of normative frameworks within which informational self-determination should take place. Informational self-determination is about individuals being in a position to participate as much as possible when it comes to accessing their information. However, these complicated policies and algorithms are incomprehensible to most people. The fact that a meaningful fulfilment of the consent requirement often becomes impossible raises the question of what additional normative checks and balances are needed. There appear to be practical and technological options to provide individuals with informational self-determination, but this is not always the case and does not apply to all types of persons.

Given the highly complex data infrastructure and the precarious status of the consent requirement by (healthcare) users, a shift in the responsibility for the relation of the user’s own information to the legislator, the regulator and designers of personalised health environments is necessary. In order to enable the careful application of informational self-determination, the responsibility of companies and government bodies will have to increase. In addition to companies, governments, and healthcare providers actively assuming their responsibilities, individuals as healthcare users must also be given the opportunity to promote informational self-determination with the help of digital tools. This could be done, for example, via a digital butler. A digital butler can automatically protect the disclosure of personal data based on user preferences in transactions between individuals and suppliers of personalised digital health environments and healthcare providers.

2. Data Protection-by-Design

The notion of data protection-by-design is closely related to the concept of privacy enhancing technologies (PET). The idea behind PET is closely linked to the principle of data minimisation and has been gradually broadened to essentially become the principle of data protection-by-design. PET is not only relevant for information technology systems but also for organisations, processes, governance and methods in general. With this applicability in mind, the concept of privacy-by-design has now become a term used worldwide. On the one hand, data protection-by-design is an obligation imposed on the data controller, while on the other it is a tool available for those who want to use its principles as an opportunity to protect themselves. This element goes beyond the obligations for the controller in the GDPR, whose duties will be discussed below.

53 ‘Privacy-Enhancing Technologies is a system of ICT that measures the protection of informational privacy by eliminating or minimising personal data thereby preventing unnecessary or unwanted processing of personal data, without the loss of the functionality of the information system’ (GW Van Blarkom, J Borking and J Olk (eds), Handbook of Privacy and Privacy-Enhancing Technologies. The Case of Intelligent Software Agents (College bescherming persoonsgegevens 2003). Ronald Hes and John Borking, Privacy-Enhancing-Technologies: The path to anonymity (rev edn, Information and Privacy Commissioner Ontario 1995).
3. Obligations of the Controller

When it comes to data protection-by-design as an obligation for the controller, Article 25 of the GDPR is relevant as it introduces ‘data protection-by-design and data protection-by-default’. A requirement of data protection-by-design is that the principle of data minimisation is respected, which includes data collected is both necessary and proportionate to the initial purpose of collection. Moreover, consideration should be given to the question of whether the personal data of everyone should be processed or if certain groups of persons could be excluded in advance. Data must also be deleted when they are collected longer than necessary. One example of data protection-by-default as an obligation for the data controller is a requirement in Japan by which the default settings of smartphones must be one that restricts signal communication. Placing default settings of smartphones to ‘automatically connect and communicate’ is still allowed in Europe, which means that the smartphone holder can be tracked permanently. In light of Article 25 of the GDPR, one could argue that the default setting of restricted signal communication in smartphones should also become compulsory.

a. Digital Butler and Algorithms

Due to artificial intelligence (AI), data protection-by-design can also contribute to informational self-determination with the help of a personal assistant, or a digital butler through a new institutional design. An example of a digital butler assisting users on privacy and data protection issues was already described as far back as 2003 in the Privacy Incorporated Software Agent (PISA) handbook. The PISA was developed with EU funds and is currently being further advanced into a digital butler that can automatically assess and handle the transfer of personal data based on the privacy preferences of the user during transactions between individuals on the one hand, and (software) providers, companies, governments and agencies on the other. One example is the Aipoly app, which can be downloaded for smartphones and utilises the phone’s camera. By focusing the camera on physical objects, the system recognizes objects, identifies the object and then displays the name of the object on the screen. This app also includes an option to vocalise the name of the object for the blind and partially sighted. Digital butlers such as intelligent software agents proposed by Borking can be privacy-enhancing only to the extent that data subjects can control the actions of the butler. Contrary to Amazon’s Alexa which is a digital assistant and not privacy enhancing. User control therefore lies at the heart of digital butlers.

In our big data society, it is often too complex for individuals to determine for themselves whether the parties they exchange their data with within a personalised health environment meet all the conditions of proper data protection. A digital butler could therefore help users to determine whether the third party can be trusted, for example, by informing the user if certain ‘credentials’ have been met.

V. Conclusions and Recommendations

The first conclusion that can be drawn is that the concept of informational self-determination has been developed both in case law and in legal publications and is now taking on a new direction as a result of the introduction and mass distribution of mobile data carriers. Informational self-determination was first and foremost a defensive ‘instrument’ to protect one’s own privacy from third parties. The term now possesses a positive and active meaning because individuals are given the freedom of choice and the opportunity to make their own decisions about what will happen to their personal data and, in the event they so desire, to manage it themselves. Furthermore, new legislation and regulations such as the GDPR, the GDPR Implementation Bills and the Act on Supplementary Provisions for the Processing of Personal Data in Care 2017 (the Dutch Provisions) are increasingly granting individuals the right to informational self-determination, such as being able to elec-
tronically review data, (informed and specified) consent, and data portability, insofar as it concerns data supplied by the data subject themselves.

The second conclusion is that social and technological developments, such as the emergence of personalised digital health environments via mobile data carriers and the use of Big Data profiling through artificial intelligence, are leading to a systematic imbalance between the power of companies and governments on the one hand and that of individuals on the other.

It is from this background, this article aimed to answer the four research questions from section II.

1. Research Question 1: Possible, Desirable and Types of Persons

Informational self-determination is principally defined as the ability of a person to determine the extent to which their personal data are used and further disclosed, for the purpose of a self-determined life. This ability to determine what personal data about them are used is influenced by:

- the emergence of personalised digital health environments through mobile data carriers, and
- the use of big data profiling by companies and public authorities that utilizes artificial intelligence.

Technological developments lead to a systematic imbalance between the power of companies and governments to hold personal data and the power of the individuals whose personal data is involved.

a. Is Informational Self-Determination Possible?

There has been a massive increase in the supply and demand of using personalised digital health environments, which seems to create opportunities for a more active and assertive shaping of informational self-determination. Although this development is still in its infancy, it could rapidly increase – as we saw with the swift success of smartphones. The enormous commercial achievement of smartphones has assisted in developing personal health environments, as there are already countless apps that make it possible to keep track and influence one’s own health.

However, it appears that for individuals, informational self-determination in an absolute sense - in which people truly have full freedom of choice and know what they are choosing and consenting to - is an illusion. Big data profiling, opaque algorithms and complex, invisible online data trade create grave imbalances. The article also aimed to highlight that people need guidance and assistance from social workers, family members and friends when exercising informational self-determination, particularly in stressful situations involving (serious) diagnoses and with people who are (physically or mentally) unable to take care of themselves. In medical literature, shared decision making is also often seen as a step towards greater patient self-determination and a more balanced patient/healthcare provider relationship. All previously mentioned research and literature are not based on an ideal of complete informational self-determination in healthcare, but rather on the changing role of healthcare providers to one of a helping hand via human or machine.

Particularly in the case of complex medical treatments, there will be interaction between the healthcare provider and the patient. It is expected that healthcare providers will focus more on complex diagnostics and joint decision making, in which personal considerations are important. In a relative implicit sense, informational self-determination seems to be increasingly possible for people who are able or willing to engage with personalised digital health environments and patient portals of healthcare providers.

German case law has shown that although the right to informational self-determination is explicitly recognised, it does not offer sufficient legal protection against drastic social and (information) technological developments. That is why in Germany the computer fundamental right has been formulated* in such a way that it aims to offer protection against the abuse of information systems.

On a European level, informational self-determination is not recognised as a right, but as an objective worth pursuing. In judicial decisions, in addition to defensive informational self-determination, active/offensive self-determination is also given more room to develop. All in all, it can be concluded that,

---

given current social, technological and legal developments, informational self-determination in healthcare is an illusion in absolute terms, but is becoming increasingly possible in a relatively implicit sense. This can be seen both in practice through the rise of personalised digital health environments, and in law through an increase of active informational self-determination rights and case law.

b. Is Informational Self-Determination Desirable?

Informational self-determination has been investigated in Germany, the Netherlands and Europe. The first to examined was Germany, the cradle for informational self-determination. Informational self-determination is a facet of the general right to personality and the right to human dignity. However, the right to informational self-determination does not appear to offer sufficient legal protection against the use of information systems. Which is why the German Federal Constitutional Court has formulated the computer fundamental right in a way that aims to offer protection against the use of information systems.

In European and Dutch law, there is no explicit reference to the right to informational self-determination, but rather an implicit one. There is European and Dutch legislation for the protection of personal data, such as the GDPR, under which processing companies and governments have obligations and individuals have rights. In Dutch legislation there are supplementary informational self-determination rights for individuals in relation to healthcare providers, but no supplementary rights in relation to processing companies and governments that process healthcare data through personalised digital healthcare environments. Yet, this additional legal protection is desirable for the sake of more informational self-determination.

c. Types of Persons

The groups of people who need legal and moral attention regarding the discussion of informational self-determination are:

- persons concerned with the abuse of power;
- persons who are unable or unwilling to 'manage' data; and
- persons who actively 'manage' their own personal data.

2. Research Question 2: Regulation

In the EU and the Netherlands there does not seem to be a general right to informational self-determination. In the Charter of Fundamental Rights of the European Union, the right to private life and the right to data protection constitute two separate fundamental rights. In Europe, in addition to the right to private life for the information society, the concept of protection of personal data has been developed.

The GDPR also accommodates separate informational self-determination rights. For personal health environments, the right to data portability is, amongst others, important. This new right is closely linked to, but different from, the right of access. The right to data portability concerns the transferability of data. It implies that the person has the right to receive the personal data that he or she has provided to a controller in a structured, practical and machine-readable form, so that they can transfer it to another controller. The purpose of this new right is to strengthen the position of individuals and give them more control. In personal health settings, the right to data portability should apply to the extent that individuals themselves provide data contained in a medical record or personalised digital health environment to the healthcare provider or digital health environment. This right is partly an incentive for the creation of personalised digital health environments, because its success depends on the ability to transfer data.

With a right to data portability of the individual concerned, the development of personalised digital health environments would contribute even more to informational self-determination. It is a new right, which still needs to be applied to real life situations. Should it prove in practice to be too restrictive - by limiting it to data supplied by the data subject themselves - for the development of informational self-determination through personalised digital health environments, legislation which aims to extend the scope of Article 20 GDPR could be considered. On the other hand, the right to data portability can also make it easier for other parties to put pressure on the data subject’s data to have access to health data in personalised digital health environments. Additional legal, organisational and technological measures to protect health data - particularly outside the healthcare context - are therefore of an even greater impor-
tance due to the right to data portability. In this sense, the GDPR itself already offers safeguards against malicious parties, but the technology neutral GDPR does not specifically consider personalised health environments.

As far as legislation is concerned, there is little or no anticipation of the advent of personalised health environments in which there are data controllers who will usually be outside the scope of the care. The legislator has not yet anticipated the increasing influence of private providers of personalised digital health environments who may increase the risk of abuse.

On the basis of the analysis in this article, my main thesis is that the developments outlined above, which give companies and governments greater power over health data, require a form of counterforce. In addition, medical privacy/confidentiality, which has traditionally applied to medical files, no longer provides any legal protection. It is to be noted that in German Criminal Procedure Law the prohibition to seize patient data has been extended to data on the Patient Card even if it not in possession of the doctor. In short, there is a need for additional regulation to actively protect individuals. Such regulation could, for example, take the form of an obligation of confidentiality and the right of data controllers to refuse to give evidence. This legislation should consider the fact that health data are to a large extent processed by controllers from outside the healthcare sector. Just like the Dutch Provisions, this legislation, which is yet to be formulated, could be complementary to the GDPR with respective international effect.

3. Research Question 3: Standardisation in Applications

As for the third research question, it turns out that standardisation can also take shape in the applications themselves, via data protection-by-design. In concrete terms, this means that when facilitating personalised digital health environments people can have the freedom of choice to access their health data in real time - at any time. In addition, a specialised digital butler can protect people in the complex big data society. Specific conditions and preferences for that unique person and unique context can be included into the butler’s code.

4. Two Recommendations for Future Developments

I will posit two recommendations for future regulation of personalised digital health environments.

a. Patient Confidentiality: Additional Duty of Confidentiality and the Right to Refuse to Give Evidence

I would argue in favour of an additional statutory duty of confidentiality for controllers of personalised digital health environments outside the treatment relationship. Such patient confidentiality must go hand in hand with the right to refuse to give evidence to suppliers and users of personalised digital health environments. As the Dutch Provisions can be regarded as supplementary to the GDPR for electronic exchange systems of care providers who process health data within the care sector, the obligation of confidentiality for data controllers of personalised digital health environments can perhaps be regulated in addition to the GDPR. Such legislation should also protect persons against third parties (municipalities, the employee, insurers) who may pressure private digital health environment users to make use of the right to a copy of their medical file in order to subsequently provide them with their health data.

b. Prohibition on Commercial Exploitation of Health Data

Finally, I call for a ban on the commercial exploitation of health data, similarly to the trade in organs being prohibited on the grounds of the Organ Donation Act. Big data profiling, opaque algorithms and complex, invisible online data trade create a systematic imbalance between the power of companies and that of individuals. Thus, the added value of a legal ban on trade in health data is beyond dispute, given the data power of companies. The exact wording of such a ban will require further investigation. Consent under the GDPR is a crucial condition for informational self-determination, but does not offer sufficient guarantees.

61 Strafprozessordnung s.97(2) 1987.