frontiers | Frontiers in Sustainable Cities

TYPE Original Research
PUBLISHED 24 August 2022
DOI 10.3389/frsc.2022.977623

Data protection as privilege—Factors to increase meaning of GDPR in vulnerable groups

Jonas Breuer[1]*, Rob Heyman[1] and Rosamunde van Brakel[2]

[1]imec-SMIT, Vrije Universiteit Brussel, Brussels, Belgium, [2]Research Group on Law, Technology and Science (LSTS), Vrije Universiteit Brussel, Brussels, Belgium

Check for updates

OPEN ACCESS

EDITED BY
Shenja Van Der Graaf,
University of Twente, Netherlands

REVIEWED BY
Eriketti Servou,
Eindhoven University of Technology, Netherlands
Ignazio Vinci,
University of Palermo, Italy

*CORRESPONDENCE
Jonas Breuer
Jonas.breuer@vub.be

SPECIALTY SECTION
This article was submitted to Innovation and Governance, a section of the journal Frontiers in Sustainable Cities

RECEIVED 24 June 2022
ACCEPTED 01 August 2022
PUBLISHED 24 August 2022

CITATION
Breuer J, Heyman R and Brakel Rv (2022) Data protection as privilege—Factors to increase meaning of GDPR in vulnerable groups. *Front. Sustain. Cities* 4:977623. doi: 10.3389/frsc.2022.977623

The General Data Protection Regulation in the EU has the potential to empower citizens towards data-based innovation and datafication. Realising this potential in practise is challenging, mainly because not everyone has the capabilities, seemingly expected by the lawmakers, to make use of relevant legal provisions. This empirical study sets out to investigate what can increase capabilities of citizens in datafied societies to understand and exercise their rights to data protection, as means to increase participation in socio-technical systems. We concentrate on vulnerable groups and criticise the GDPR as regarding data literacies as intrinsic life goals instead of instrumental means. We expand vulnerability to capability deprivation, based on a dynamic understanding of layered vulnerabilities. This overcomes solely negative associations of vulnerability and provides a more constructive framing in support of literacies of everyone, including less literate or more vulnerable. Based on this approach, we consider what is lacking to achieve GDPR literacy. We conducted interviews with representatives of civil society organisations supporting different groups in Flanders, Belgium. Based on these insights, we argue that a layered approach to vulnerability leads to a layered approach to capabilities, and to a layered approach of support based on the most appropriate conversion factors for different groups: (a) at the right place and time, (b) broader support structures from authorities, and (c) a focus on clear communication with the reader in mind.

KEYWORDS

data protection, vulnerability, empowerment, capabilities, data literacy, datafication

Introduction

Datafication—the conversion of social action into online quantifiable data that enables real-time tracking and predictive analysis (Mayer-Schönberger and Cukier, 2014)—is happening all around us. The ways we move are monitored and analysed by means of information gathered along the way (Van der Graaf, 2018; Sourbati and Behrendt, 2021). The lives and communications we have are steered and facilitated by social networks and data-driven platforms (Van Dijck, 2014; Van Raemdonck and Pierson, 2021). Jobs are regulated by algorithms and their makers (European Commission Joint Research Centre, 2018; Rosenblat, 2018). Data is being processed in public spaces to make our cities "smart", to improve urban life and governance (Morozov and Bria, 2018; Cardullo et al., 2019; Vandercruysse et al., 2020). Much of the underlying data is controlled by high-tech companies and commercial interests (Powell, 2014; Ruppert et al., 2017). A big share of the data is (or can become) so-called personally identifiable, which links up to the active debate around data protection (Edwards, 2016; Loideain, 2019).

The General Data Protection Regulation in the EU [*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)*, 2016], or at least some of its provisions, are argued to be more than a compliance procedure in data-driven projects: a framework to empower citizens regarding innovations that are based on their personal data (Grafenstein, 2019; Ritsema van Eck, 2019; Christofi et al., 2022). Realising this potential of the General Data Protection Regulation (GDPR) in practise is, however, challenging. Despite positive efforts, not everyone can make use of the regulation: understanding complex technical systems and legal provisions is a privilege of experts, and can be near impossible for others. This is the hypothesis underlying this work, that there is a mismatch between expectations implied in European data protection law and the capabilities of citizens. The main question of the empirical study presented here is therefore: how can the capabilities of citizens to understand and exercise their rights to data protection be increased, to increase participation in socio-technical systems?

In answering this question, we concentrate on vulnerable groups. We question whether vulnerability is the right conceptual frame and criticise the GDPR and data literacy as proposing literacies as intrinsic goals instead of instrumental means to achieve more open-ended goals. We expand vulnerability to capability deprivation (Sen, 2001; Robeyns, 2005) to illustrate how knowledge, motivation, and skills are necessary to consider GDPR as an answer to different challenges in datafied societies. Based on the capability approach (Sen, 2001; Robeyns, 2005), we consider what is lacking to achieve GDPR literacy. The main concept is the conversion factor: environmental, social, and personal factors required to exercise rights for meaningful participation. Answering the research question in this way will, we hope, contribute the emergence of smarter and more just communities.

In order to understand what factors aid or constrain the use of the GDPR we conducted interviews with representatives of civil society organisations representing different vulnerable groups: older people, gig economy workers, adults with low education, people in poverty and others. We identify current challenges of those groups and how these might be related to the GDPR. For example, sharing economy freelancers wish to understand the way an algorithm decides on pricing or routing. Data subject access requests could help address this need. Then, we consider what can be changed on environmental, social, and personal conversion factors to overcome the identified challenges.

In the following, the article first provides a theoretical discussion of empowerment in the GDPR and the notion of vulnerability before we introduce the capability approach. Then, after describing the utilised methodology, we dive into the empirical data of the interviews and discuss our insights.

The promise of empowerment

Empowerment is about autonomy and self-determination, "the capacity of individuals, groups and/or communities to take control of their circumstances, exercise power and achieve their own goals, and the process by which, individually and collectively, they are able to help themselves and others to maximise the quality of their lives" (Adams, 2016). With datafication comes "the power to gather, aggregate, process, store and act upon data extracted from the flows of everyday life" (Couldry, 2020, p. 1136). Those with that power can influence and interact with society, how it is organised and functions, and how that has an effect on individuals' daily lives. In the GDPR, the actor with that power is called data controller [GDPR, Art.4(7)] and is obliged to ensure compliance with the law.[1]

Empowerment in the legal framework of data protection promises to give individuals the power to know and determine risks with regard to data protection rights and their potential mitigative actions (Ausloos, 2020). We should note that empowerment in the GDPR is limited to the definition of risks to data protection rights and mitigating actions to those risks. The notion of risks to fundamental rights and freedoms is essential here (van Dijk et al., 2016).

Prior to an innovation's implementation or launch, risks with regard to data subjects'[2] rights can be determined with a data protection impact assessment (DPIA). During the life of an implemented innovation, data subjects can exercise rights to identify and mitigate risks with regard to their personal data. These are the GDPRs main instruments of empowerment. DPIAs assess, prior to a processing, whether it "is likely to result in a high risk to the rights and freedoms of natural persons"

[1] The data controller is the main decision-maker that exercises overall control over the why and how personal data is being processed. UBER, for example, is the data controller in relation to all processing of personal data on their ride-hauling platform, of both the drivers and the passengers.

[2] Data subjects are persons whose personal data is being processed according to GDPR, Art.4(1).

[GDPR, Art.35(1)] and to "seek the views of data subjects" [GDPR, Art.35(9)]. Academic literature[3] stress the significance of involving different stakeholders during a DPIA (Wright, 2012; van Dijk et al., 2016). In practise, little of this is happening and data subjects remain a silent or implicated actor (Breuer and Pierson, 2021). Without involvement or representation the power remains with the controller. We focus on the rights in this article because they are not facultative as is participation in DPIAs. Furthermore, as those in charge of DPIAs already struggle to consult data subjects, it seems unlikely that extra efforts required to reach vulnerable groups would be taken.

Consent and data subject rights (GDPR, Chapter III) are the traditional legal tools that enable control and empowerment (Lynskey, 2014). These rights aim at informational self-determination of data subjects (Thouvenin, 2021). They also intend to ensure access to information about processing of personal data, its purposes and actors involved (e.g., transparency and informed consent requirements) and to the data (e.g., right of access). Their effectiveness is called into question when data processing becomes both more ingenious and pervasive (Ausloos, 2020) but also because the regulation seems to imply knowledgeable users/data subjects that have the capabilities to exercise their rights (Ausloos and Dewitte, 2018). Moreover, from a legal point of view, the protection of personal data is understood primarily as a form of individual right, and an individual challenge (Cohen, 2019). However, when investigating empowerment and socio-technical practises, it becomes clear that experiences and risks of new technologies are often collective. Capabilities and expectations of privacy are subjective and context specific, and datafication and digitalisation can work both in empowering and disempowering ways, perceived differently by different persons and groups.

These instruments for data subject empowerment embody some noteworthy shortcomings: the supreme power of controllers, the implied capabilities of data subjects and the individual focus on data protection rights. By default, data subjects are expected to know and be able to exercise their rights. Razzano (2020) rightfully argues that individualised privacy self- management strategies, as implemented by the GDPR, are problematic as the sole (or chief) model for data protection. And, while it can be challenging for non-experts to understand how to take self-determined decisions regarding complex technical systems and legal provisions, it can be near impossible for less informed people. The extent to which these rights are granted thus depends on personal characteristics of people, their perceptions and capabilities. There is a mismatch between data protection law and abilities of citizens; concerning both the actual processing of their personal data (e.g., purposes or who has access to it) and the protection afforded by the GDPR (e.g., data subject rights).

Vulnerability, literacy, and the GDPR

This section discusses the notion of vulnerability in relation to data protection rights. Subsequently, we argue that the capability approach is more appropriate both for the objective of this study and for constructively using data protection rights to strengthen the position of disempowered groups in datafied societies.

There are several issues regarding the conceptualisations of vulnerable data subjects. First, the concept of vulnerable data subjects is under-conceptualised. Only recently more attention is being paid to these issues within academic personal data protection research. It seems that narrow definitions of vulnerability describe a specific issue related to a specific group, which is then defined through implementing acts. These acts or their implementation seem to close the discussions of other forms of vulnerability. The question arises whether vulnerability is the right concept at all. Second, the approach taken within the law is not intersectional, socio-economic factors are not considered as variables that render a data subject vulnerable. Third, the focus in these discussions on risks has the consequence that less attention is given to empowering effects of data collection and processing. For instance, registrations in the context of police helps to assess the extent of ethnical profiling. Finally, in practise data protection authorities (DPA)[4] seem to have not taken up the issue yet for vulnerable data subjects apart from providing recommendations and guidelines with regards to children.

The notion of vulnerability does not only describe actual harms that have come to a person but also the "susceptibility to certain sorts of harm" (Goodin, 1985) thus the potentiality of harm (Gilson, 2014). Being vulnerable—across different legal sectors—generally means being more exposed to harms (if compared to other individuals) in certain contexts (Peroni and Timmer, 2013). Pierson (2012) differentiates between external vulnerability (exposure) vs. internal vulnerability (coping) in relation to privacy. But there is no single definition.

In the GDPR the term vulnerability is mentioned explicitly only once (Recital 75). It explains that risks to the rights and freedoms of natural persons that could lead to physical, material, or non-material damage may result from processing. This may concern, among several other aspects, personal data

[3] DPIAs were only introduced by the GDPR and are "a newcomer in the impact assessment vocabulary" (van Dijk et al., 2016) but were not a new approach because they are, like older privacy impact assessments, models of ex ante risk analysis to evaluate future impact of a service or product on privacy or data protection.

[4] DPAs are independent public authorities that oversee the application of data protection law through investigation and corrective powers (Art. 51 GDPR). They offer expert advice and investigate complaints alleging violations of the GDPR and other national laws. Each EU member state has at least one.

of vulnerable natural persons, in particular children. The recital does not go into detail. Some legal scholars argue that the emphasis is purposefully placed on children requiring particular attention without excluding other categories of vulnerable people (without being explicit) (Piasecki and Chen, 2022). All data subjects could therefore be considered as potentially vulnerable with regards to the collecting and processing of their data and their relationship to the data controller.

Malgieri and Niklas (2020) argue that this universal perspective of vulnerability has downsides as important differences between data subjects could be ignored, thereby exacerbating already disadvantageous positions of some. They term this the "universality-particularity dichotomy" (Malgieri and Custers, 2018, p. 7), whether everyone is equally vulnerable or some more than others. Another dichotomy significant for data protection practises is about the manifestations of vulnerability: arising within the data processing (decisional vulnerability risks, e.g., due to lack of literacy) or as a consequence of it (some data processings can cause for example discrimination) (Malgieri and Niklas, 2020, p. 7). The challenge is, according to these authors, whether the protection framework should focus on harms or on procedural safeguards, both of which have disadvantages.

Towards dynamic applications of vulnerability

To overcome some of these issues, Malgieri and Niklas (2020) suggest a layered approach to vulnerability based on Luna (2009), which resonates with the capability approach we will come back to below. Luna argues that layers of vulnerability are traits created by status, time, and location, rather than fixed attributes of certain persons or groups. Layering, in this sense, opens the door to a more intersectional approach and emphasises cumulative and transitory characteristics. Vulnerability is a universal human condition, but varies from person to person with varying degrees of intensity, and influenced by a variety of situations. Drivers on the UBER platform, for example (see the Section Results for more information) are mostly non-native speaking immigrants that may have difficulties finding other work. Working at UBER, then, constitutes another layer of vulnerability because here they are prone to discrimination by untransparent rules of the platform. Their negotiating position is already weak due to previous layers and working conditions will not easily be changed. Criticising or complaining might cost their jobs, which is yet another layer.

Malgieri and Niklas (2020) argue that this layered approach to vulnerability is in line with the risk-based approach adopted in the GDPR, "i.e., everyone is potentially vulnerable, but at different levels and in different contexts" (Malgieri and Niklas, 2020, p. 9). The risk-based approach supports a layered study of vulnerability because the GDPR's concept of risks for fundamental rights corresponds to the concept of vulnerability as higher risks of damages for some individuals. It can help identify and understand various risks (and layers) that potentially magnify, expose, and exploit various vulnerabilities. Returning to DPIAs as a potential site of empowerment, the operationalisation of layered vulnerability depends on the contextual understanding of the controller that is assessing the risks.

Data literacy

In this section we turn to the notion of data literacy as a positive capacity to do something contrary to decisional vulnerability, the "lack of awareness and understanding of consequences and legal rights" (Malgieri and Niklas, 2020, p. 8). We extend the discussion to data literacy as it focuses on two dimensions not present in vulnerability conceptualisations; personal autonomy and motivation to change power relations.

Pangrazio and Sefton-Green (2020) refer to individual actions to control personal data. Carmi et al. (2020) refer to goals that could be achieved with data literacy. According to the former, data literacy is about the way "individuals might better engage with and make use of the 'personal data' generated by their own digital practises" (Pangrazio and Sefton-Green, 2020, p. 420). "Personal data literacies" focus on: (1) data identification, (2) data understandings, (3) data reflexivity, (4) data uses, and (5) data tactics. Carmi et al. (2020) provide a broader definition where data literacy is empowerment to challenge existing power asymmetries. "Data literacy means understanding and being able to challenge, object and protest contemporary power asymmetries manifested in datafied societies". They call this "data citizenship" which consists of the areas of (1) data thinking (citizens' critical understanding), (2) data doing (everyday engagements with data), and (3) data participation (proactive engagement with data and networks of literacy) (Carmi et al., 2020). Data subject rights (and the transparency obligation in the GDPR) allow the five domains of Pangrazio personal autonomy that could lead to data citizenship and motivations to change power relations.

The GDPR then becomes a key set of principles that provides instrumental means to achieve these forms of data literacy through its implementation. The two definitions show that there can be a focus on the GDPR as an intrinsic goal or as a tool for different goals that go beyond the GDPR. Here, the capability approach helps to understand why literacy or vulnerability approaches to the GDPR should consider the regulation as an extrinsic goal; to make use of one's personal data and as a means to achieve other goals.

Beyond vulnerability

The different perspectives above consider either a lack of capacity to control personal data or the capacity to control personal data, or motivations for doing so. A lack of control has been defined as a risk or a vulnerability and is more narrowly related to the GDPR and specific demographic attributes such as age. But the same vulnerability was also defined more broadly as different layers that may contribute to an incapacity to control with or without the GDPR. The capacity to control data has been described as data literacy and this consists of actions that individuals may undertake to assert control over their personal data. For literacy, we can also discern a perspective where such control is seen as an intrinsic goal or as a means to reach broader goals. The link with the GDPR is less explicit but the regulation offers these means in the form of data subject rights. Contrary to layered vulnerability, data literacy does not explain what factors contribute to data literacy.

We propose to combine the two perspectives of vulnerability and literacy because both separate perspectives present different factors to consider (a lack or a presence of) control over personal data. The underlying question in vulnerability is, what is causing a specific vulnerability; traits created by status, time, and location. For data literacy the causes that were given relate to personal motivation. One can become data literate for an intrinsic goal, to control one's personal data; or an extrinsic goal, to challenge power asymmetries related to personal data. When combining both, acting data literate depends on traits created by status, time, and location. This rings true because a person's status should consider their education and thus their potential knowledge of the GDPR and data subject rights. Status alone does not explain a data literate action, people require the right time and place to act on their data subject rights. Max Schrems could be seen as a person with the right status (a student learning about data protection), location and time to investigate his data protection rights and infringements for Facebook. His status is significant, but he also had time and was in the right place to receive support to do what he did. We also want to consider the role of motivation as a factor that could be added to vulnerability. People may choose not to use their rights, and this may put them at a risk. For example, you decide to simply trust a party with your data without reading a cookie disclaimer, a practise that occurs more often than not.

In conclusion, we may consider vulnerability and data literacy on a continuum where vulnerability is linked to a lack of capacities to control data and data literacy is linked to a capacity to control data (see Table 1). If this is the case, we can say that the combined literature considers personal aspects, contextual aspects, and motivational factors to explain either vulnerability or literacy but not both. In line with Gilson (2014), among others, who criticises solely negative associations of vulnerability, we suggest the capability approach as a more constructive framing in support of literacies of everyone, including the less literate or more vulnerable based on a dynamic understanding of layered vulnerabilities.

Capability approach

On the shared spectrum of vulnerability and data literacy, the capability approach offers a better understanding of factors that shape these capabilities on an individual level, and how this individual's capacities are influenced by social and environmental factors. The latter will allow us to better answer what can be improved with regard to the GDPR's implementation context so that people are less vulnerable, more in control and have the capacity to choose to exert their rights if they so choose.

Key concepts

The basic tenet of the capability approach is that empowerment should measure what people are able to achieve (Sen, 2001). As a tradition in development studies this contradicts approaches that measure empowerment as having access to rights or commodities. "Being able to achieve" implies a distinction between what people have realised and what they could realise. What people have achieved as meaningful goals or states of being are called *functionings*. What people are possibly able to achieve are *capabilities*.

Functioning

What people have achieved in terms of attainable achievements or states of being. If people are aware of the GDPR and how to apply the knowledge, they may achieve the function of being data literate. If we naively assume that this is the case for all Europeans, then we can also observe that not all Europeans choose to achieve this function. Being able to communicate through social media and not wanting to read lengthy privacy statements illustrate that people may have other functionings they wish to achieve first.

Instrumental functioning

This category of functionings enables other functionings. Being well-fed or having a roof over your head are functionings of a special sort. These allow other achievements. Most people will need the latter two to start to study in order to obtain a degree. So, it is possible to list certain functionings as instrumental to reach other functionings. For example, understanding the GDPR is instrumental to challenge surveillance capitalism by enforcing data subject rights.

TABLE 1 Continuum from vulnerability to data literacy.

Focus	Risks or vulnerabilities	Literacy or actions
GDPR and data	GDPR vulnerability is a static risk that should be considered by a data controller in a DPIA for specific demographics	There are possible actions to assert control over personal data (some can be found in data subject rights)
Broader than GDPR	Multiple reasons outside the GDPR lead to non-use of the GDPR, such as power imbalances, traits created by status, time, and location	Data literacy is a tool to challenge bigger societal challenge such as power imbalances

Capabilities

Capabilities are best defined as potential functionings. They are what people are able to achieve but have not yet. For some Europeans that understand the GDPR and how to apply it, having data protection rights is a capability. It could potentially be achieved but as illustrated earlier, this also depends on other meaningful goals in a person's life.

Motivation and individual differences

The differentiation between capabilities as a potential and functionings as an achieved goal is key in this approach. It allows us to move away from a paradigm where all people are treated or defined as having equal opportunities as individuals. For example, some people may decide not to use the GDPR because they find another life goal more important, such being able to use a service without reading the small print. This also shows that there are people with different needs; not everyone needs the same level of data protection due to their personal circumstances and preferences. To explain why someone is able to use the GDPR or not we need to look at conversion factors and capability deprivation, respectively. These two concepts explain if capabilities are available to a certain individual or not.

Conversion factors

Conversion factors are what stands between a capability and a functioning. These factors "influence how a person can convert the characteristics of the commodity into a functioning" (Robeyns, 2005, p. 99). While Robeyns refers to commodities, rights can also be converted to a functioning (Britz et al., 2013). Sen discerned five factors that influence the conversion of a good into a functioning. These are the personal, environmental, social climate, relational and familial factors (Britz et al., 2013). Robeyns discerns three types: personal, social and environmental. To reduce complexity we will continue with Robeyns' three conversion factors.

Mapping the conversion factors for an individual would answer whether a person has access to a certain capability set and thus is able to achieve a certain functioning. On a personal level, being data literate and aware of data subject rights could both be seen as good examples of a personal conversion factor. Data literacy overlaps with personal conversion factors. At the environmental level, having access to all relevant information to formulate a data access request would be a good example. And lastly, we could consider a support network that helps someone to have access to relevant information and that helps formulate a specific request as an example at the social level.

Capability deprivation

Capability deprivation is a situation where an individual lacks conversion factors for a certain capability set. Due to this lack, it is impossible for this individual to achieve the desired functioning. In the case of the GDPR, not being able to read a privacy statement could be seen as an example of a missing personal conversion factor. A social conversion factor that is lacking could be that a person does not have access to a support network. Lastly, environmentally, a power imbalance might exist between a data controller and data subject where a data subject might decide that the benefits of a GDPR-intervention do not outweigh other risks that fall outside the scope of the GDPR, for example losing one's job.

In conclusion, if we compare Table 2 below to Table 1, we can see how the capability approach offers a more balanced framework to look at vulnerability and data literacy. By evaluating whether specific people have the capability to act data literate, it will also be clear who is deprived of this capability. The factors that explain capability deprivation or a capability are the two sides of the same coin. These are personal, social and environmental factors. We should also note the key idea underlying the difference between a capability and functioning. People may have the potential to act data literate because they have social support and an environment where one is free to act on the GDPR, but they may still have other priorities to convert this data literate potential into a data literate action. People may refrain from doing so because they value other things more than control over their personal data.

Methodology

In this article, we set out to determine conversion factors, following the capability approach (Sen, 2001; Robeyns, 2005), that can support empowerment of citizens in datafied societies through the data protection rights in the GDPR. The main research question of this study is what can be done to increase the capabilities of urban dwellers to understand and exercise their rights to data protection to increase participation in socio-technical systems?

We interviewed experts working for Belgian civil society organisations that represent different vulnerable groups in two iterations. The interviewees include among other representatives of a labour union, of organisations for adult education, poverty, digital skills of citizens, an anti-discrimination and equality body, and a legal communication agency (a full list with details can be found in subsequent section).

Interviewees in the first iteration were selected based on a short questionnaire about expectations of Flemish citizens regarding the protection of their data and privacy. It was sent to twenty-two organisations in Flanders and Brussels. The contacted organisations represent different disempowered and vulnerable groups and were contacted as members of the "Task force for E-inclusion in Flanders[5]." This selection ensured prior engagement with and interest in the topic as well as a range of target groups. Eleven representatives of ten organisations responded to the survey, of which six were willing to be interviewed. On the basis of these interviews, we identified current challenges of vulnerable groups and how these might relate to the GDPR. To go more into depth, we wanted to consider what concretely would need to be done to increase understanding and adoption of the instruments the GDPR offers. We contacted more experts to identify what can be changed on the environmental, social, and personal conversion factors to increase adoption of the challenges identified in the first round. For this second iteration, we interviewed three relevant representatives. A full list of the organisations can be found in Section Interviewee background.

The interviews were semi-structured and were conducted online *via* Microsoft Teams (six were conducted in Dutch, three in English) and transcribed non-verbatim with the software F4transkript. The analysis was structured by four themes, which also provide the structure for the next section: background of interviewees, capability deprivations, capabilities, and conversion factors.

Results

In this section, we start with describing the different organisations, the work they do and their target groups. We then untangle their input by considering, first, GDPR functionings that we could identify based on the interviews; second, characteristics of their target groups to better understand what capability deprivation means in the reality of their work; third, the capabilities that were mentioned (i.e., what their target groups are able to do with the resources they have access to, if conversion factors are present). This serves mainly to understand what is keeping people from making more use of their rights and freedoms anchored in the GDPR. Last, we report conversion factors that were discussed, i.e., how a person can be or is free to convert the characteristics of the resources into a functioning.

Interviewee background

United Freelancers is part of the Belgian trade union ACV (Algemeen Christelijke Vakbond van België) and represents freelancers and all independent workers without employees (dutch: ZZP'ers) in Belgium. We interviewed the national representative of the organisation and talked about the Deliveroo riders and UBER chauffeurs they support. Their angle is labour law. The criteria that platforms use to make decisions are based on data processing, personal data protection regulation seems to offer significant advantages for them (with a view towards discrimination of the workers).

Seniorennet Vlaanderen is a non-profit organisation that supports others like associations, municipalities, or libraries in providing digital skills to older people without any or very little prior knowledge. We interviewed the president of the organisation to talk about their target group, which usually does not voluntarily use the technology/services or learn about it. Seniorennet teaches basic skills such as how a smartphone works or using email and WhatsApp. For this target group, data protection is very removed from their realities. Discussing these topics with them is difficult due to the gap in knowledge, skills and interest according to the interviewee. They are happy if they can use WhatsApp.

LIGO[6] offers diverse trainings for adults with low education regardless of their native language to increase their chances in society. We interviewed the data protection officer of the organisation, who does not have direct contact with the target group. Data protection was not an explicit part of the e-inclusion track that the organisation offers to the students at the time of the interview.

VOCVO is a support organisation focussing on literacy, learning in detention and clear language. We interviewed the coordinator of the "Strategic plan for literacy" of the Flemish Government. As coordinator between different organisations that focus on providing knowledge and skills to low educated adults, they are positioned between target groups, organisations and objectives but have no direct contact with any students.

Netwerk Tegen Armoede is a network of various organisations working for and with people in poverty. We

[5] https://e-inclusie.be/taskforce

[6] Ligo was called Federatie Basiseducatie at the time the interview was conducted.

TABLE 2 Capability approach as a framework to for vulnerability and data literacy.

Capability deprivation			Conversion factors		
Negative power imbalance	**Lack of support**	**Age, literacy, awareness**	**Data literacy**	**Data literate support**	**Balanced or positive power imbalance**
Environmental	Social	Personal	Personal	Social	Environmental

talked to the general coordinator of the organisation. Data protection is not necessarily a priority in their work but can be useful as a means to an end, not least because administration for people in poverty obviously involves lots of personal data.

Mediawijs is a non-for-profit organisation that supports Flemish citizens, especially younger ones, in navigating the digital world, in gaining the digital and media literacy necessary to do so. They are mainly targeting other intermediaries with the right knowledge and means to target their own target groups: teachers, libraries etc. We interviewed the general coordinator.

Helderrecht is an agency that helps to communicate in plain and understandable legal language. We talked with one of their legal designers, who is implementing design thinking in the legal world, which is relatively new and uncommon. The agency has an own method for plain legal language, giving trainings and support to two target groups: social workers working with people on a daily basis and need practical, legal advice (e.g., how to remove personal information from the internet); and legal professionals (e.g., judges or the Belgian Data Protection Authority) to make their communication more accessible. This work is not limited to data protection.

UNIA is the national human rights institution and equality body in Belgium, with a narrow mandate on discrimination and promoting equality. They provide trainings and policy advice, do case handling and strategic litigation. This is done in three domains: labour, criminal law, and public sphere (education, health, insurances). In each domain, UNIA has strategic partners (trade unions, law enforcement, civil society organisations). Data protection is not part of the mandate (primarily data protection related questions are referred to the DPA) but can be useful when a clear link exists with their mandate. It will gain importance for their work with increasing significance of AI in equality debates.

AVANSA is an adult education centre in Flanders that organises formations, activities, workshops, lectures, etc. on a broad range of topics. We interviewed the head of the digital education section in one Flemish city. They work mostly with adults that seek additional education, mainly middle-class people that are getting older (50+) and/or need some support in a digitalised society.

Functionings

As discussed above, according to Sen and Robeyn, functionings are capabilities that have been realised based on capability sets. In our study, we consider GDPR functionings as intrinsic goals. In the interviews, we investigated among others what kind of GDPR functionings exist among their target groups. In general, it seems that the topic of data protection rights might be too much to consider for (some of) them, who might not have the means, the skills, or the interest to understand and consider them in their daily life. It seems that many people don't have the capabilities that are expected to exercise data protection rights. Some of the discussed groups are experiencing other struggles that are often enormous barriers to being able to participate in society.

The interviews illustrated that individualised privacy self-management strategies, as implemented by the GDPR, are a problematic model for data protection. Intermediaries (e.g., teachers, public servants, relevant authorities, policy, and lawmakers) are required to support data subjects; whether they are not able or not interested in participating. Yet also data controllers and intermediaries do not seem to have sufficient knowledge to properly support data subjects or to know themselves what acceptable risks are. For example, teachers that use certain platforms to organise their online classes. Another example is how the GDPR grants rights to data subjects, but this often boils down to data controllers that are afraid of getting sued instead of aiming at empowering those whose data they process. Yet another example is legal experts who may not be able to help others to understand what is at stake, as discussed with the legal designer. The interviews also highlighted the importance of personal data processing and sharing in certain situations, and the clear and tangible benefits that can arise therefrom.

Capability deprivations

A broad range of "capability deprivations" were discussed with the interviewees. This helped us to better understand the layered nature of vulnerabilities (or deprived capabilities). Deliveroo riders and UBER drivers, for example, are deprived of power vis-a-vis the untransparent and unaccountable platform.

It controls them, manages, follows them and decision-making criteria—automated decisions that mean earning an income or not—are not known. Nor is it known exactly what kind of data is being processed by the platform when taking those decisions. This results in a strong power asymmetry. As the interviewee of the trade union explained, a majority of this group also has a migration background, and may not speak the official languages of Belgium. The policy officer of the human rights institution explained that although there may be an emphasis on possibilities to claim rights *via* administrative and judicial channels, there is still a high threshold for the many to benefit from these procedures (e.g., to contact the data protection authority). The representative of the adult education centre explained that the most vulnerable groups may not even be able or interested to access basic information (going to a library or joining classes with others can already constitute barriers).

These examples demonstrate how different vulnerabilities exacerbate power asymmetries. And, being disempowered to start with causes additional deprivations. Different layers of vulnerability overlap and reinforce each other. For example, people in poverty feel that they do not have the same rights because they are in a weaker position already. What is more, to get the help they require, they need to agree to disclose even more data. This disclosure can be untransparent due to issues such as not being fluent in an official language or feeling intimidated by long texts written in legal jargon. Some ways of providing information, such as providing long texts in difficult administrative or legal language, actually creates more barriers instead of facilitating understanding.

For people with little education and low literacy in general, provision of information and translation of knowledge becomes even more challenging, again creating layered deprivations along the way. The representative of *VOCVO* explained how for low-literate adults, the digital world can be too much. Concerns predominate and are often a reason to not start participating or learning the required skills. This results in the dilemma that on the one hand they need to participate while on the other hand they are scared by what they hear, and they lack the skills to start learning. Without digital skills, it has become almost impossible to participate in our society, and that makes the digital gap even bigger (e.g., during Corona many lessons could only take place digitally).

The representative of *SeniorenNet* explained that the struggles their target group is experiencing are preoccupying: where can I do my banking if the branch in my village closes, how do I interact with my municipalities that are digitising services etc. Also, there is fear related to feelings of helplessness. The interviewee explained how small changes in user interfaces, e.g., of Google, and buttons in new locations are already a main source for confusion. There remains little space of mind to worry about personal data processing.

Capabilities

A person's "capability-set" denotes the set of achievements or functionings that he or she can choose from given their situation. In this section, we describe some capabilities of the groups discussed during the interviews. For example, the organisation providing trainings to elderly without any digital skills does not teach data protection rights in their classes. It would be too complicated, technical, and thus ineffective for the target group according to the interviewee. The representative of the adult education centre explained that their target group is satisfied with doing some things better (e.g., using an adblocker and do-not-track services) rather than alternative software solutions that could make a bigger difference (to e.g., Apple and Google) according to them. The user friendliness is too big an argument.

The representative of the labour union explained that their target groups are very interested in knowing more about decision-making criteria and what data is being collected: are they being discriminated against, and if so, how, and why? This would allow the workers to adapt their behaviour, which would not be in the interest of the corporations. However, the interviewee doubted that there is much interest in using data protection rights to improve this situation.[7] This supposed lack of interest seems to stand in contrast with the possibilities the GDPR theoretically offers. The right to access, for example, could be a means of pressure in favour of the workers (this seemed to be the data protection right most interesting for the interviewee). This apparent lack of interest might be because they are data subjects deprived of certain capabilities: they do not know their rights, they don't speak the language of the country they work in, they stay for only 4.3 months on average with one of these two platforms. This very temporary nature, on the one hand, might be a reason why the workers are not interested and, on the other hand, reinforces their weaker position towards the platforms.

According to the representative of the adult education centre, many of their students are uninterested, resigned, but also cynical about their lack of power towards the big companies that process their data: why should they worry if they cannot do anything. They further considered it possible that the age category of the target group may have something to do with this attitude, or possibly cultural characteristics of the populace. When asked why the data protection rights do not appear useful in the context of these arguments, they explained that their target groups are feeling so inadequate towards the data processing technologies that they are defensive and feel incapable of taking a more assertive stance: "these people are not Max Schrems".

Information is key but determining the most effective way of conveying complex information can be very challenging. People

[7] In the UK, the NGO Worker Info Exchange has successfully taken action against UBER by using the GDPR provisions. See www.workerinfoexchange.org for more information.

in poverty feel that they are being insufficiently or unclearly informed according to our interviewee. They know little about the data that is being shared among institutions, or rights they have regarding their personal data (for example the right to access and the right to rectification). The use and sharing of data can be perceived as done against their interests, to control and sanction them. The interviewee explained that there is the interest in more insights through better communication, to be empowered to contribute to the discussion around the processing of their personal data. And there are also advantages to some data sharing, for example for pro-active and automatic granting of rights (e.g., using personal data to better refer people to the right services), but also less paperwork and less required proofs.

One interviewee explained that a pragmatic approach to data protection that highlights both advantages and risks is most constructive. Clear and transparent communication of which can add to the capability sets of disempowered people.

Another interviewee argued that not everyone should have to be interested in data protection issues. People may not want to be obliged to think about these, they have other concerns and others should take care of it for them. They expect that data is collected and used only for the purpose they are aware of (e.g., loyalty cards) and do not think they should expect this not to be the case. They do get worried when they hear about misuses etc. and then it turns into a negative feeling, also a feeling of a lack of control. Furthermore, the interviewee discussed that he feels that the individual rights are related to an individual guilt model, where it is an individual's responsibility that no misuse or other risks take place. "Expecting that people can act and fight for privacy, with legal processes etc. is a very legalistic viewpoint of society."

The interviews have shown in this regard that the capability sets of their representatives and people that aim at supporting them is at least as important as their own. For example, despite the potential that data protection rights can help platform workers in their struggle for empowerment, the interviewed representative doubted the added value of data protection legislation compared to labour law. Without specific expertise, it can be very challenging to realise capabilities and civil society organisations are certainly required as an intermediary for disempowered groups to do so. Also the intermediaries struggle, for example teachers that are not trained in data protection legislation (and why would they). Training and support for those intermediaries is key. The human rights body, for example, chooses strategic partners in different domains (e.g., labour unions) to which they provide the knowledge for further dissemination.

Conversion factors

As was mentioned before, conversion factors influence how a person can convert a capability into a functioning. Robeyns (2005) distinguishes conversion factors on three levels: personal (e.g., being literate and aware), environmental (e.g., access to all relevant information) and social (e.g., a support organisation). In this section we will discuss the conversion factors that we have learned during the interviews. We aim to identify environmental, social, and personal conversion factors to increase the effectiveness of data protection rights in empowering citizens.

Personal conversion factors

The first level of conversion factors are personal ones: factors that influence how a person can convert the characteristics of a capability into a functioning. Being able to convert capabilities into an achieved functioning is far from straightforward. For example, the anticipation that one will not be able to understand something (e.g., small letters and privacy notices) may be a barrier to trying in the first place. One interviewee explained how this can be a survival strategy: not opening letters and bills if you cannot read the text, avoiding a problem instead of dealing with it. One of the interviewees suggested that focussing on the most deprived groups in the efforts to create adequate conversion factors is the best approach, because most people would benefit not least because every data subject can be (come) vulnerable in interaction with certain technologies and companies.

Several of the interviewees also discussed how some discussions around privacy create fear: phishing, Facebook, identity theft etc. This can function as an argument to not realise capabilities. Certain ways of providing information can thus actually cause converse effects, creating fear and barriers instead of helping people to realise a functioning. Overcoming such fears would thus be a first conversion factor. But sensibilisation is complicated: know the dangers, how to handle them but also know the benefits and advantages. One interviewee said that the target groups would not actively seek help or increase their digital skills themselves. The information should be disseminated at the moment when the people are struggling with a concrete problem. For example, at the town hall patient support is provided when faced with e-government affairs.

Along similar lines, the adult education centre provides information on data protection in the context of concrete tools and challenges (for example when teaching a service such as Google Photos), rather than trajectories focussing exclusively on the topic or on advanced tools for privacy management (the interviewee mentioned Nextcloud as an example). This makes the issue of data protection less scary but it also resonates more with the capabilities of their target group. Again, it was stated that a balanced story between benefits and risks is most conductive. Still, as the story of the older people with no digital skills at all illustrates how for certain groups personal conversion factors are inexistent and support is required.

Environmental conversion factors

The second level of conversion factors according to Robeyns are environmental ones, which we understand here as access to information. One interviewee, representing people in poverty, thinks it is appropriate to discuss data sharing on a regular basis. It must be clear which data is shared with whom and why. In some situations, data is also shared between certain authorities without a concrete assistance program. In those cases, people in poverty want to explicitly be consulted whether the data may be passed on. As mentioned before, it is decisive in what manner the information is conveyed. Heated debates in the media, for example, can have the adverse effect of creating more fear.

Two of the organisations that were interviewed focus on a very important aspect in this regard for their target groups but in general, namely clear communication. This especially addresses the organisations that offer digital services. For example, small letters and privacy notices are impossible to comprehend for people with low literacy. This creates a feeling of having to accept something that you do not understand at all. The organisations that are enacting digitalisation should keep the barriers low to ensure accessibility. An example given by the interviewee was the unemployment agency, where an email address and password are required as a first step to even start finding work. Here, the problems can already start when one does not understand the concept of email/password. This is very important in the context of e-government and banking, which are essential for being a part of society. Another interviewee referred to Nutriscore,[8] which is an attempt to simplify the nutritional rating system and give information on the overall nutritional value of food products. They argued that the information here is so simple and accessible that it become insufficient. Another example of an interesting manner to convey information and thus create conversion factors is a package for secondary schools developed by the organisation *Mediawijs* to raise literacy, in a more playful manner (an example given was a friend's book with a privacy notice). This package has been developed in cooperation with the Flemish data protection authority.

One of the interviewees works for a legal communication agency that focuses on plain legal language, a method adopted from design thinking to the legal world, where this is far from common to date. The idea is that complex legal texts are translated into language that others than legal experts can understand. In other words a user-centric method ("empathy for the readers") to make information understandable, which could be decisive for realising the potential of data protection rights. As positive as this idea can be, the challenge is to ensure that texts stay legally correct while being more accessible. The interviewee explained how, depending on the information, combinations of techniques and visuals, always with the reader in mind, are utilised in their method. They further explained that the balance between correctness and accessibility is often a barrier for those that have the responsibility, who may rather stick to the original text than take any risks. Unfortunately, this way of making information more accessible also takes much more time.

Social conversion factors

The third level of conversion factors are social ones, which we understand as support from other people or organisations. As has become clear on previous pages, all organisations of which we interviewed representatives aim at providing conversion factors to their target groups, although most may not focus directly on data protection and related rights. Each is focussing on specific needs of their target groups. An underlying goal is to foster, stimulate and coordinate so that citizens can actively and critically use the media, including people that are at the margins of society and those that are not interested. One interviewee argued that for them it is important to regard citizens not only as consumers in this context but also creative participants.

The labour union, for example, actively and directly supports Deliveroo riders and UBER drivers towards the powerful platform companies. The adult education centre raises the general awareness of their staff and teachers to adapt their lessons to include the most important data protection aspects without overwhelming their students. The organisations supporting adults with low education are very aware that the already difficult translation of expert knowledge becomes more challenging with their target groups. Also here, teachers are trained as intermediaries that are not necessarily experts in data protection but experts in working with the needs of this target group. To support this target group, the interviewee stated that it is most important to provide the information and education at the right moment and right location. For example, the classes do not focus on digital skills but address all kinds of skills, which is perfect because they have the right tempo and there is familiarity with the environment/teacher/group. Feelings of safety and trust can be necessary for conversion. This is generally important according to the interviewee. Existing organisations should be activated, trained and streamlined instead of creating other, parallel tracks.

The centre for plain legal language offers trainings to intermediaries, like legal professionals, to make their work more accessible. The human rights body provides other sorts of support, too. One of their activities is strategic litigation, to clarify unclear rules or give more progressive interpretations of certain criteria (examples of intersectionality, multiple discrimination were given and the right to meaningful information). Moreover, they train people and operate a database with situations to recreate. This helps in claiming rights *via* administrative and judicial channels. However, as valuable as these activities are to, they do not target 'normal' citizens and are certainly not accessible to people with little capability sets in

[8] Nutriscore is being used in several European countries at the time of writing this article.

the context of data protection rights. This is also the case with data protection authorities, who are required to offer advice to any organisation or citizen but are difficult to reach even for professionals. At least the one in Belgium also seems to have too little resources to do their work satisfactorily.

Discussion

While it may seem obvious that some GDPR functionings lack in disempowered groups because of capability deprivations, the important question for this empirical research is how to enable people to become more empowered in a digitalised world, and whether the GDPR can be a useful instrument in this regard. As we discussed in the theoretical section above, we used the capability framework of Sen to find concrete answers. Capabilities are what people are able to do with the resources they have access to. Capability sets constitute all feasible functionings available to a person (Sen, 2001, p. 75), including freedom of choice. Individuals can still decide not to convert a possible functioning into an achieved functioning (motivational exclusion instead of factual). In this article, we set out to empirically identify and understand conversion factors that could increase the likelihood of GDPR adoption in datafied societies.

Instead of the notion of vulnerability, which negatively indicates a lack of something, we argue that framing situations of asymmetric power relations for data subjects as capabilities (or a lack thereof) is more conducive to finding practical solutions. For example, rather than assuming that poor people lack the capability to understand what is happening with their data, one should consider how to discuss benefits and risks with them constructively (i.e., provide conversion factors).

We frame vulnerabilities as capability deprivation: where conversion factors lack, and due to this lack it is impossible to achieve a desired functioning. For example, Deliveroo riders wish to understand the way an algorithm decides on pricing or routing. Data access rights could help address this need. But they often do not speak the main language of the platform they are working for, are a low-income workforce and earning a salary is more urgent than data protection. Their asymmetric relationship with the powerful platforms does not support them in learning, understanding, and applying something as abstract as data protection rights. To circumvent such capability deprivation, conversion factors can be provided (as shown in Section Results). It is important to note, however, that not all capabilities can be realised or are desired to be realised. For example, the power imbalance between data controller and data subject is so that the subject might decide that the benefits of a GDPR-intervention do not outweigh other risks that fall outside the scope of the regulation. In the case of the platform workers, losing one's job could be a retribution for unwanted behaviour.

In other words, people may have other problems. The situation of older people exemplifies this. Concepts such as data protection rights are far away from the everyday lives that they have very little impact. Awareness, knowledge, and skills regarding data processing (i.e., data literacy) are often low in the groups of data subjects that were discussed in the course of this study. Fear is one aspect for the lack of capabilities: fear of misdeeds, of authorities or generally of knowing that you do not have the skills to do what is required of you. Still, the study has also demonstrated that in the concrete contexts and related to specific needs, anyone may potentially get interested and can become able to get involved in that specific situation, for example UBER drivers wanting to know algorithm decision criteria or adults that use a service such as Google Photos.

The layered approach to vulnerability, as was discussed above, leads us to a layered approach to capabilities, or layered capabilities as conceptualised by Sen and Robeyn. The next logical step, then, is to also consider a layered approach to offering support based on different capability sets and the most appropriate conversion factors for different groups.

First, people with limited capability sets regarding data protection rights should not be expected to actively seek support themselves. As was mentioned before, lack of awareness, fear or shame are among the reasons for this. Luckily, a lot of support providing conversion factors is out there although the offer of data protection rights related aspects remains limited. In order to address this issue, it seems important that support is provided where and when it is needed, in relation to the specific situation a data subject may find itself in. This means that general awareness campaigns about abstract risks, rights and freedoms (which might, to be honest, be a rather dry topic for many) are less useful. It seems most helpful to use (existing) structures and intermediaries that are already known and trusted. In this regard, it seems most important to train the intermediaries. Some of the organisations discussed above already offer such services.

Second, it seems indispensable that also at a higher-level support is being provided that may not be directed at citizens themselves but at those intermediaries. After all, any citizen should be able to not be interested and still be protected. This support needs to come from policy makers, municipalities, and relevant authorities. The human rights body discussed above illustrates how important this can be. Regarding data protection aspects, the various data protection authorities that exist in each member state should take up much more active roles, which so far is not the case in Belgium. As they seem to be struggling with their mandates, one may consider whether they could, instead of becoming more accessible themselves, at least provide concrete guidelines, knowledge, and other support for the supporters (work together with a number of strategic partners for example). A supportive intermediary or a lack thereof has not been included in the consulted literature about GDPR vulnerability or data literacy, while it is key according to our research. As was mentioned before, little guidelines exist on how vulnerable data subjects can be involved or even about what the notion entails. This also relates to the argument above that the GDPR's emphasis on individual rights and responsibilities are a problematic model for data protection if not backed by communitarian structures, from teachers to civil society organisations to experts to relevant authorities to policies and supporting laws.

Third, and maybe most essential, is the very broad conversion factor of accessible language/communication. One of the organisations offers a centre for clear language addressing specifically low-educated adults. But this aspect is clearly not limited to what one might consider vulnerable data subjects. Many citizens do not understand privacy notices or are not aware of what might be happening with their (personal) data behind the scenes of processing operations. Approaches and methods of clear/plain legal language, for example as discussed above, are extremely valuable and it is a very positive development if they gain momentum in the legal world.

Conclusion

Doubtlessly, our dependency on technology is almost ubiquitous today. Much of it has a data processing component. Rights to data protection are supposed to protect and empower all citizens in datafied societies with regards to the processing of their personal data. Our hypothesis for this work was, however, that there is a mismatch between expectations in data protection law and the capabilities of citizens. We laid out above that indeed, the assumption of knowledgeable data subjects with the capabilities to exercise their access rights, as implied by the GDPR, is debatable.

We started off with the notion of vulnerable data subjects. As argued in Section Vulnerability, literacy, and the GDPR, there are several issues with its conceptualisation. Regarding the lack of academic research in this context, we think that framing vulnerabilities rather as (a lack of) capabilities as suggested above seems to be the better approach to finding answers. This consideration could complement promising legal research by some scholars (Gianclaudio Malgieri is a notable example in this regard), also to facilitate intersectional legal approaches to vulnerable data subjects. Another aspect that we could confirm during our study is that the focus on risks in relevant debates often overshadows the positive and empowering aspects of data processing. Both should be considered and carefully balanced, which is in fact in line with the GDPR's risk-based nature, which does not intend to inhibit all processing but to assess risks in relation to benefits, including the perspectives of data subjects. The interviews discussed above confirm that at least in Belgium, the relevant authorities should provide more guidelines on vulnerable data subjects and how the rights of them can be guaranteed. Alone, the GDPR's recital 75 about risks to the rights and freedoms of natural persons seems confusing rather than helpful.

With our empirical study, we set out to answer the question: what can be done to increase the capabilities of citizens to understand and exercise their rights to data protection, to increase participation in socio-technical systems? The focus here was on conversion factors, not to change the GDPR but to point out what could be changed in the context between this framework and specific users. We suggest a layered approach to conversion factors, which acknowledges different layers of capabilities and is open to consider everyone's specific situations and possibilities. Expectations regarding personal data processing cannot be generalised, are context-dependent and need to be understood in context-specific ways. This includes not being interested in the topic and expecting safeguards beyond the individualised exercise of rights. The three layers of support can be summarised as (a) at the right place and time, (b) broader structures not least to ensure the rights of those unmotivated, uninterested or incapable, and (c) a focus on clear communication with the reader in mind.

For future research on vulnerable data subjects and empowerment through data protection, especially in the legal domain, it seems most important to (re-)consider the role of the data protection rights and the GDPR in general. The research presented here illustrates that the regulation and its provisions may not be intrinsic goals of the general populace. Knowing exactly about what our data protection rights are is only interesting for a few people. These rights are tools to achieve other goals that go beyond the GDPR but that can be essential in many situations, to be or become a self-determined and proud member of datafied societies.

Data availability statement

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Ethics statement

Written informed consent was obtained from the individual(s) for the publication of any potentially identifiable images or data included in this article.

Author contributions

JB and RB conceived the design of the study. RB provided the background for the vulnerability part. RH contributed the conceptualisations of the capability approach. JB organised the empirical study, analysed and reported the data. JB and RH contributed to the discussion and conclusion. All authors contributed to the article and approved the submitted version.

Funding

This work was supported by the regional science foundation of Flanders in Belgium as strategic basic research in the form of the 4-year Interdisciplinary Research Project SPECTRE (SBO Project No. S006318N). More information and contact details can be found under spectreproject.be.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Adams, R. (2016). *Empowerment, Participation, and Social Work*. New York, NY: Routledge.

Ausloos, J. (2020). *The Right to Erasure in EU Data Protection Law: From Individual Rights to Effective Protection*, 1st Edn. New York, NY: Oxford University Press.

Ausloos, J., and Dewitte, P. (2018). Shattering one-way mirrors – data subject access rights in practice. *Int. Data Privacy Law* 8, 4–28. doi: 10.1093/idpl/ipy001

Breuer, J., and Pierson, J. (2021). The right to the city and data protection for developing citizen-centric digital cities. *Inform. Commun. Soc.* 24, 797–812. doi: 10.1080/1369118X.2021.1909095

Britz, J., Hoffmann, A., Ponelis, S., Zimmer, M., and Lor, P. (2013). On considering the application of Amartya Sen's capability approach to an information-based rights framework. *Inform. Dev.* 29, 106–113. doi: 10.1177/0266666912454025

Cardullo, P., Di Felicaiantonio, C., and Kitchin, R. (2019). *The Right to the Smart City*, 1st Edn. Bingley: Emerald Publishing.

Carmi, E., Yates, S. J., Lockley, E., and Pawluczuk, A. (2020). Data citizenship: rethinking data literacy in the age of disinformation, misinformation, and malinformation. *Internet Policy Rev.* 9, 1–22. doi: 10.14763/2020.2.1481

Christofi, A., Breuer, J., Wauters, E., Valcke, P., and Pierson, J. (2022). "Data protection, control and participation beyond consent-'seeking the views' of data subjects," in *Research Handbook on EU Data Protection*, eds E. Kosta and R. Leenes (Cheltenham: Edward Elgar Publishing).

Cohen, J. E. (2019). Turning privacy inside out. *Theor. Inquiries Law* 20, 1–31. doi: 10.1515/til-2019-0002

Couldry, N. (2020). Recovering critique in an age of datafication. *New Media Soc.* 22, 1135–1151. doi: 10.1177/1461444820912536

Delete (2016). 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), (April 27, 2016).

Edwards, L. (2016). Privacy, security and data protection in smart cities: a critical EU law perspective. *Eur. Data Protect. Law Rev.* 2, 28. doi: 10.21552/EDPL/2016/1/6

European Commission and Joint Research Centre (2018). *Platform Workers in Europe: Evidence From the COLLEEM Survey*. Publications Office. Available online at: https://data.europa.eu/doi/10.2760/742789 (accessed July 28, 2022).

Gilson, E. C. (2014). *The Ethics of Vulnerability: A Feminist Analysis of Social Life and Practice*, 1st Edn. London: Routledge.

Goodin, R. E. (1985). *Protecting the Vulnerable: A Reanalysis of Our Social Responsibilities*. Chicago: University of Chicago Press.

Grafenstein, M. (2019). "Co-regulation and the competitive advantage in the GDPR: data protection certification mechanisms, codes of conduct and the 'state of the art' of data protection-by-design," in *Research Handbook on Privacy and Data Protection Law. Values, Norms and Global Politics*, eds G. González-Fuster, R. Brakel, and P. De Hert (Edward Elgar Publishing). Available online at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3336990 (accessed July 28, 2022).

Loideain, N. N. (2019). A port in the data-sharing storm: the GDPR and the Internet of things. *J. Cyber Policy* 4, 178–196. doi: 10.1080/23738871.2019.1635176

Luna, F. (2009). Elucidating the concept of vulnerability: layers not labels. *Int. J. Feminist Approaches Bioethics* 2, 121–139. doi: 10.3138/ijfab.2.1.121

Lynskey, O. (2014). Deconstructing data protection: the 'added-value' of a right to data protection in the eu legal order. *Int. Compar. Law Q.* 63, 569–597. doi: 10.1017/S0020589314000244

Malgieri, G., and Custers, B. (2018). Pricing privacy – the right to know the value of your personal data. *Comput. Law Secur. Rev.* 34, 289–303. doi: 10.1016/j.clsr.2017.08.006

Malgieri, G., and Niklas, J. (2020). Vulnerable data subjects. *Comput. Law Secur. Rev.* 37, 105415. doi: 10.1016/j.clsr.2020.105415

Mayer-Schönberger, V., and Cukier, K. (2014). *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, 1st Edn. Houghton, MI; Boston, MA; New York, NY: Mariner Books, Mifflin Harcourt.

Morozov, E., and Bria, F. (2018). *Rethinking the Smart City: Democratizing Urban Technology*. Rosa Luxemburg Stiftung. Available online at: https://onlineopen.org/media/article/583/open_essay_2018_morozov_rethinking.pdf (accessed December 8, 2021).

Pangrazio, L., and Sefton-Green, J. (2020). The social utility of 'data literacy'. *Learn Media Technol.* 45, 208–220. doi: 10.1080/17439884.2020.1707223

Peroni, L., and Timmer, A. (2013). Vulnerable groups: the promise of an emerging concept in European Human Rights Convention law. *Int. J. Constitut. Law* 11, 1056–1085. doi: 10.1093/icon/mot042

Piasecki, S., and Chen, J. (2022). Complying with the GDPR when vulnerable people use smart devices. *Int. Data Privacy Law* 12, ipac001. doi: 10.1093/idpl/ipac001

Pierson, J. (2012). Online privacy in social media: a conceputal exploration of empowerment and vulnerability. *Commun. Strateg.* 4, 99–120. Available online at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2374376

Powell, A. (2014). "'Datafication', transparency, and good governance of the data city," in *Digital Enlightenment Yearbook 2014: Social Networks and Social Machines, Surveillance and Empowerment*, 215–224.

Razzano, G. (2020). *Understanding the Theory of Collective Rights: Redefining the Privacy Paradox*. Available online at: https://researchictafrica.net/wp/wp-content/uploads/2021/02/Data-Trusts-Concept-Note.pdf (accessed July 28, 2022).

Ritsema van Eck, G. J. (2019). "Algortithmic mapmaking in 'smart cities': data protection impact assessments as a means of protection for groups," in *Good Data*, eds A. Daly, S. K. Devitt, and M. Mann (Groningen: Institute of Network Cultures), 298–316.

Robeyns, I. (2005). The capability approach: a theoretical survey. *J. Hum. Dev.* 6, 93–117. doi: 10.1080/146498805200034266

Rosenblat, A. (2018). *Uberland: How Algorithms Are Rewriting the Rules of Work*. Oakland, CA: University of California Press.

Ruppert, E., Isin, E., and Bigo, D. (2017). Data politics. *Big Data Soc.* 4, 205395171771774. doi: 10.1177/2053951717717749

Sen, A. (2001). *Development as Freedom*, 1st Edn. New York, NY: Anchor Books.

Sourbati, M., and Behrendt, F. (2021). Smart mobility, age and data justice. *New Media Soc.* 23, 1398–1414. doi: 10.1177/1461444820902682

Thouvenin, F. (2021). Informational self-determination: a convincing rationale for data protection law? *J. Intellect. Property Inform. Technol. Electron. Commerce Law* 12, 246–256. Available online at: https://www.jipitec.eu/issues/jipitec-12-4-2021/5409 (accessed August 11, 2022).

Van der Graaf, S. (2018). In waze we trust: algorithmic governance of the public sphere. *Media Commun.* 6, 153. doi: 10.17645/mac.v6i4.1710

Van Dijck, J. (2014). Datafication, dataism and dataveillance: Big Data between scientific paradigm and ideology. *Surveil. Soc.* 12, 197–208. doi: 10.24908/ss.v12i2.4776

van Dijk, N., Gellert, R., and Rommetveit, K. (2016). A risk to a right? Beyond data protection risk assessments. *Computer Law Secur. Rev.* 32, 286–306. doi: 10.1016/j.clsr.2015.12.017

Van Raemdonck, N., and Pierson, J. (2021). "Taxonomy of social network platform affordances for group interactions," in *2021 14th CMI International Conference - Critical ICT Infrastructures and Platforms (CMI)*, 1–8.

Vandercruysse, L., Buts, C., and Dooms, M. (2020). A typology of smart city services: the case of data protection impact assessment. *Cities* 104, 102731. doi: 10.1016/j.cities.2020.102731

Wright, D. (2012). The state of the art in privacy impact assessment. *Computer Law Secur. Rev.* 28, 54–61. doi: 10.1016/j.clsr.2011.11.007