Conceptualizing Autonomy in an Era of Collective Data Processing

Graef, Inge; Petročnik, Tjaša; Tombal, Thomas

Published in:
Digital Society

Publication date:
2023

Document Version
Publisher's PDF, also known as Version of record

Digital Society (2023) 2:19
https://doi.org/10.1007/s44206-023-00045-3

ORIGINAL PAPER

Conceptualizing Autonomy in an Era of Collective Data Processing: From Theory to Practice

Inge Graef[1,2] · **Tjaša Petročnik**[1,2] · **Thomas Tombal**[1,2]

Received: 1 September 2022 / Accepted: 17 April 2023

Abstract

While literature has already recognized the relational and collective impact of data processing, there is still limited understanding of how this affects the design of legislative instruments. We submit that legislators must recognize trade-offs between one's own interests, the interests of other individuals, and collective or societal interests more explicitly in regulating data. To frame our analysis, we rely on a two-fold definition of autonomy as a notion that inherently requires positioning oneself within a broader context with others. While the inward-looking dimension of autonomy focuses on the ability of an individual to make free and independent decisions in her own interests, the outward-looking dimension considers the relationship of one's choices with other individuals' and collective interests.

Building on this working definition of autonomy, we assess three legislative instruments, namely the General Data Protection Regulation, the Digital Markets Act and the Data Act proposal, to identify to what extent this multi-dimensional nature of autonomy is reflected in the design of data-related obligations. We examine how legislators can make trade-offs between different interests explicit and thereby bring the regulation of data more in line with the current societal reality that is increasingly dominated by relational and collective effects of data processing.

Keywords Autonomy · Data protection · Data regulatory initiatives · Relational and collective interests

✉ Inge Graef
i.graef@tilburguniversity.edu

Tjaša Petročnik
t.petrocnik@tilburguniversity.edu

Thomas Tombal
t.j.a.tombal@tilburguniversity.edu

[1] Tilburg Institute for Law, Technology, and Society (TILT), Tilburg University, Tilburg, The Netherlands

[2] Tilburg Law and Economics Center (TILEC), Tilburg University, Tilburg, The Netherlands

Published online: 13 May 2023

1 Introduction

EU data protection law is built on the idea that individuals should have the right to control how personal information relating to them can be communicated to others (Westin, 1967). The EU General Data Protection Regulation ("GDPR": Regulation (EU), 2016) has as one of its core objectives to protect individual data subjects (Graef & Van der Sloot, 2022: 519–521), which is evidenced by the rights to access, erase and port personal data that data subjects hold in certain situations (GDPR: Art. 15, 17, 20). However, because one's data often also contains insights about others, decisions about the use of one's personal data can affect the ability of others to control what insights are available about them. For instance, the testing of one's DNA can also reveal information about the health of one's relatives who may not want to become aware of these insights (Hallinan et al., 2013). Examples like this one make clear that one cannot always fully control what information is collected or processed about oneself.

To some extent, the GDPR acknowledges the fact that decisions of individuals can have impact beyond their own particular interests. Beyond rights for individual data subjects, the GDPR also creates more pre-emptive and structural rules that must be respected by data controllers, such as making the latter responsible for complying with the data protection rules through the principle of accountability (GDPR: Art. 5(2)), or requiring them to integrate data protection by design and by default in the way they build their products or services, to conduct data protection impact assessments in certain situations, or to appoint Data Protection Officers ("DPOs") (GDPR: Art. 24, 35, 37). That being said, those measures and rules imposed on controllers nevertheless mainly have as focus the individual data subjects, which they aim to empower. This has consequences for the way autonomy and self-determination as overall objectives of European data protection law can be interpreted.

In the era of big data and data analytics, the collective impact of data processing is becoming increasingly pronounced. This brings the limits of the focus on individuals even more to the fore. Focusing solely on the individual is unlikely to capture the impact of data analytics practices enabling companies to draw inferences or profile groups of people beyond the control of that individual, but nonetheless affecting them (Bietti, 2020; Reviglio & Alunge, 2020, 596; Taylor et al., 2017). Literature has increasingly recognized this collective impact of data processing. De Brouwer (2020) argued that the protection of one's privacy is inherently interdependent on choices made by others. Viljoen (2021) emphasized the fundamentally relational aspect of data collection by referring to how personal data identifies relationships between individuals. In economic terms, the processing of personal data creates externalities implying that choices regarding the collection of one's personal data have external effects on others, which are typically not considered in personal data sharing decisions (Acemoğlu et al., 2019).

Despite attempts in literature to conceptualize the collective nature of the use of personal data and AI technologies (Mantelero, 2016; Taylor et al., 2017; Smuha, 2021), the current regulatory framework still emphasizes the individual

as the locus for protection and sometimes overlooks the collective effects of data processing. Collective interests are mainly protected as a sum of individual issues, based on individual rights (Reviglio & Alunge, 2020: 599). This does not reflect the current reality in data-driven markets where data use has effects beyond the individual level and is often outside of the individual's sole control.

Again, the GDPR itself also recognizes to a certain extent this relational and collective impact of data processing, as it envisages the necessity to find trade-offs between conflicting interests in some of its provisions. This is due to the fact that it also has as core objective to promote the free movement of personal data within the EU internal market (GDPR: Art. 1). This is notably visible from the possibility for data controllers to process personal data on the basis of legitimate interests which override the individual interests or fundamental rights and freedoms of the data subject's whose data are being processed (GDPR: Art. 6(1)(f)). It is also visible from the way in which the data portability right has been designed (GDPR: Art. 20), which we will analyse later in this paper (see Section 3). However, while the GDPR makes room for such trade-offs, we will argue that it does not go far enough in considering collective interests. This is because although some GDPR provisions invite to consider the interests of others and collective interests, it does not protect these interests as such. Indeed, such concerns are only "activated" when an individual interest is at stake, and, as we will see below (see Section 3), they are quite limited.

Moving beyond the GDPR, this paper will illustrate that two other related European legislative initiatives, namely the EU Digital Markets Act (Regulation (EU), 2022a) and the EU Data Act proposal (Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data), may in fact equally disregard the trade-off between individual and collective interests in some of their provisions. The reason why we focus on these two instruments, rather than on others, is twofold. On the one hand, they both impose *compulsory* obligations on market players restricting how they can use data, like the GDPR and unlike the Data Governance Act ("DGA": Regulation (EU), 2022b), which only lays down conditions for the implementation of *voluntary* mechanisms to use and exchange data in the form of data intermediation services and data altruism (DGA: Art. 10–25). On the other hand, the way one's own, other individuals' and collective interests are treated in the Digital Markets Act and the Data Act proposal leads two completely opposite outcomes, which makes their comparison interesting. Indeed, as we will illustrate in Section 3, the Digital Markets Act arguably overlooks the interests of others and the collective interest, while the Data Act proposal arguably overlooks the interests of the individual.

As a core message, this paper submits that legislators must recognize trade-offs between one's own interests, the interests of other individuals, and collective or societal interests (such as democracy, public health, fostering competition and innovation, or the protection of the environment) more explicitly in developing regulatory mechanisms relating to the use of data in order to better account for the relational and collective impact of data processing. In some cases, this may result in not every individual actor's choice being upheld in order to achieve certain societal or collective objectives.

By leaving these trade-offs unnoticed, regulation can in our view not adequately reflect the reality in which data processing takes place. This does not mean that the

interests of the individual no longer deserve to be prioritized, but more awareness of the interaction with the interests of others and collective interests is needed for legislators to make more informed decisions about how to let our data-driven society develop. Depending on the circumstances and the policy objective pursued, either the individual's interests, or the interests of other individuals, or the collective interests should get priority. In this regard, we will argue that the collective impact goes beyond the sum of the interests of the individuals involved in a certain data processing activity — for instance, when one individual opts in to receive a more personalized service to the benefit of herself and other users who value personalization, but the collective interest in competition may suffer because additional data is brought under the control of the same company.

Against this background, the paper contributes to existing literature by proposing a concrete conceptualization of autonomy in light of the relational and collective impact of data processing and by testing its application in the context of three legislative instruments regulating data. The objective is to explore whether and to what extent the existing legislative framework concerning data processing can support a more relational and collective reading of autonomy and what lessons can be drawn for future legislation. The choice for autonomy as overarching concept stems from its multi-dimensional nature, which inherently requires positioning oneself within a broader context with others and thereby makes it particularly suitable to reflect on the need to reconcile different interests. In this regard, the multi-dimensionality of autonomy points to the existence of "different dimensions, which cannot all be maximised simultaneously" (see Wittrock, 2022: 1122, discussing the relations between liberal nationalism and religion). Beyond this, our contribution can be situated in debates that see data as a shared resource, a *commons*, and address the social dilemmas that pertain to it (see Hess & Ostrom, 2007: 3). In our case, the relevant dilemma is how to regulate the use of data as a resource taking into account one's individual interest, other individuals' and collective interests.

Based on a selection of literature discussing how to situate the individual in relation to others (including feminist, communitarian, public health, and environmental ethics approaches), Section 2 proposes a working definition of autonomy that is defined by reference to its inward- and outward-looking dimensions. While the inward-looking dimension focuses on the ability of an individual to make free and independent decisions in her own interests, the outward-looking dimension considers the relationship of one's choices with other individuals' and collective interests. This twofold definition of autonomy acknowledges that multiple interests are at play that need to be traded off against each other, as illustrated above with genetic data.

Section 3 assesses the three legislative instruments imposing compulsory obligations on market players restricting the way they can use data, namely the GDPR, the Digital Markets Act and the Data Act proposal, to identify to what extent the multi-dimensional nature of autonomy drawn from theory is or can be reflected in practice in interpreting and implementing key data-related obligations. In this regard, the paper examines (1) the extent of control and responsibility an individual has over the protection of her personal data (the inward-looking dimension of autonomy); (2) the limits that other individuals' and collective interests pose to the exercise of control and responsibility by an individual (the outward-looking dimension of autonomy);

and (3) if relevant, how such balancing of interests takes place and by whom. By doing so, we explore how legislators can make trade-offs between different interests explicit and thereby bring the regulation of data markets more in line with insights from literature and the current societal reality that is increasingly dominated by relational and collective effects of data processing.

2 Autonomy and Data Processing: Perspectives from the Literature

2.1 Understanding Autonomy in Relation to Data Processing Practices

In relation to (personal) data processing, autonomy has traditionally been interpreted in an individual-centric way, in the sense that "controlling and manipulating information and data about oneself is an exercise of 'self-determination'" (Rouvroy & Poullet, 2009: 51). What is envisaged here is individuals' capacity to make decisions on all aspects of their life and "to resist social pressures to conform with dominant views" (Rouvroy & Poullet, 2009: 46; Sunstein, 2003: 157–158). As a result of this traditional interpretation, "in a context of pervasive possessive individualism and at a time where private property and the laws of the market are perceived as the most efficient ways to allocate rights, the right to 'informational self-determination' has increasingly been understood as implying a sort of alienable property right of the individual over his personal data and information" (Rouvroy & Poullet, 2009: 51). Yet, for Rouvroy and Poullet (2009: 51), this is a misunderstanding of this concept, as "the "self" is not merely irreductible but also essentially different from "data" and "information" *produced about it*. […] This is an important point to recall today, as personal data have become *proxies* for persons" (emphasis in the text).

Said otherwise, the individuals' right to autonomy and informational self-determination should not only be understood as their ability to decide which data they share with whom, but also, and more fundamentally, as their right to understand and exercise control on who has their data, what is being done with it and how this impacts their life and their possibility to exercise their autonomy by making their own choices (and acting upon them); as opposed to being subject to decisions made about them on the basis of personal data used as proxies and over which they might not have control (Rouvroy & Poullet, 2009: 56; Delacroix & Veale, 2020: 82). Indeed, it is fundamental to take into account the "individuals' capacity for not doing or wanting everything which they are "statistically" predisposed to do or want, and to always assert their right to themselves to account for their own motivations" (Rouvroy, 2016: 37). Some forms of opacity are indeed necessary to sustain the individuals' self-determination and autonomy (Rouvroy & Poullet, 2009: 58).

Yet, as both public and private actors increasingly rely on ever-more invasive observation and monitoring technologies (big data, AI,…), as "more invasive industries are emerging to process data collected from sensors in homes, environments, and even on our bodies" (Delacroix & Veale, 2020: 80), and as we shift towards a "(capitalism) surveillance society" (Zuboff, 2019) and a "datafication of society" (Dencik et al., 2018), individuals, who are asked to share more and more data, become increasingly

transparent and lose this opacity (Rouvroy & Poullet, 2009: 45–46). As a result, they are increasingly subjected to (semi-)automatic decisions taken on the basis of the constant observation of their choices, behaviours and emotions, and therefore become "decreasingly capable of living by their fully autonomous choices and behaviours" (Rouvroy & Poullet, 2009: 47). Indeed, with the further development of these profile-based computing technologies (e.g. the emergence of "Emotional AI") our "ability to resist or contest this extraneous [statistical] definition [of ourselves], already under pressure, will be increasingly compromised" (Delacroix & Veale, 2020: 84). Consequently, there is a clear risk that "we will end up conforming to the profile-based, extraneous definition of ourselves, thus turning such profiles into self-fulfilling prophecies" (Delacroix & Veale, 2020: 85; Hildebrandt, 2015: 71–72).

Importantly, protecting an individual's autonomy is not only necessary for the individual itself, but also, more critically, for the collective interest "in preserving a free and democratic society" (Rouvroy & Poullet, 2009: 55; Dworkin, 1988). Accordingly, the individuals' autonomy should not be conceived "as a liberty held in isolation by an individual living secluded from the rest of society but, on the contrary, as a right enjoyed as member of a free society" (Rouvroy & Poullet, 2009: 57), as will be further examined below.

Therefore, it would be ill-advised to solely take an individual approach of autonomy without considering its necessary collective component. Indeed, if this collective approach is overlooked, "the empowerment of individuals with regard to their personal data risks being interpreted as making the satisfaction of individuals' immediate preferences with regard to their personal data, their choice to keep it undisclosed or to commodify personal information a *final value*" (Rouvroy & Poullet, 2009: 50 – emphasis in the text). This while an individual's decision to reveal (or not to reveal) data will not only have an impact on her own autonomy, but also on others' autonomy. This is because the increasingly sophisticated technologies that are used to process growing amounts of data exploit the relational and collective nature of data (Rouvroy, 2018: 429), as the focus is no longer on the individuals as such, but rather on their relations with one another and the profile they correspond to (i.e. their "statistical doppelganger") (Rouvroy & Berns, 2013: 168).

Indeed, when an individual shares data about her own behaviour, habits and preferences, this also reveals significant information about her friends, family, neighbours as well as about any other people having similar characteristics (Acemoğlu et al., 2019: 1). This can be illustrated by the infamous Cambridge Analytica scandal, where the data disclosed by 270,000 users of the "This is your digital life" application allowed Cambridge Analytica to infer detailed information about more than 50 million Facebook users and to use these insights to send targeted political messages to these Facebook users in order to influence the Brexit referendum and the 2016 US presidential election (Acemoğlu et al., 2019: 1; Chang, 2018; Granville, 2018). This example, which is only the tip of the iceberg, reveals that the core nature of predictive big data is to rely on data shared by individual samples in order to forecast the characteristics or behaviour of groups (Acemoğlu et al., 2019; see also Reviglio & Alunge, 2020: 596). It also reveals that we can no longer afford to put an excessive focus on individual rights, while broadly overlooking other individuals' and collective interests.

Data sharing by an individual creates externalities (Fairfield & Engel, 2015; MacCarthy, 2011), as it also reveals information about other individuals whose information is correlated with hers, even if they themselves did not share any data (Acemoğlu et al., 2019: 36–37). This is depicted by Ben-Shahar (2019) as a phenomenon of "data pollution". Therefore, an individual's autonomy is influenced by disclosure choices made by others, as "protecting one's data becomes increasingly costly the more others reveal about themselves" (Acquisti et al., 2016: 5). This can be highly problematic, as these externalities might lead towards excessive data sharing situations, where individuals decide to overlook their own preferences by sharing more data than they would have wanted to, because they know that the fact that others have broadly shared their own data will already have revealed much information about them (Acemoğlu et al., 2019: 1). Furthermore, if data analytics can draw inferences from a representative sample of others' data, tools focused on individual's control like consent effectively lose its meaning anyway (see Nissenbaum & Barocas in Reviglio & Alunge, 2020: 608).

Furthermore, these externalities can be enhanced by the fact that when individuals are asked to divulge large quantities of data about themselves in order to be provided with more personalized choices, there is a risk that those data could be further disseminated with other actors, such as data brokers. While the GDPR should in theory prevent this from happening, due to the purpose limitation and data minimisation principles (GDPR: Art. 5(1)(b) and (c)) and the duty to extensively and clearly inform data subjects about the processing of their personal data (GDPR: Art. 12 to 14), the fact remains that, in practice, there are strong informational asymmetries. Individuals "have no direct interaction with these data brokers, [and] they have no way of knowing the extent or nature of the information collected and sold for a multitude of reasons including fraud prevention, marketing and credit scoring" (Rouvroy, 2016: 8). This is fundamental to keep in mind because, due to these asymmetries of information "consumers are rarely (if ever) completely aware about privacy threats and the consequences of sharing and protecting their personal information" (Acquisti et al., 2016: 3). Often, they will not know exactly which data will be used, for which purposes and whether these processing are truly necessary (Rouvroy & Poullet, 2009: 68). Moreover, "personal data may be used to influence individual decision-making in subtle, targeted, and hidden manners, raising questions over the limits of a person's autonomy and self-determination in a world where so much personal data can be gathered and used to influence the individual" (Acquisti et al., 2016: 44; Calo, 2014), and the opacity of these decision-making systems greatly limit their contestability by individuals (Delacroix & Veale, 2020: 80–81).

As a result, there can be a tension between retaining one's own autonomy over whether to share personal data, and other individuals' and collective interests that may be harmed by an individual's decision relating to data processing. The collective interests go beyond the sum of the interests of the atomized individuals involved and can also affect society at large (Smuha, 2021: 3–4; see further Rodwin, 2010: 617–8). For this reason, individuals cannot be reasonably expected to take collective interests into consideration. For instance, even though individuals may not want to share sensitive personal health data for research purposes due to privacy concerns, the collective interest in effective healthcare may dictate that such personal data

is still used with certain safeguards in place. Because individuals will inherently tend to act in their own interests and those individuals' interests will not always be aligned with the collective interest, there is a role for legislation to anticipate the protection of the collective interest — as we will discuss in Section 3.

2.2 Proposition for a Working Definition of Autonomy that also Embraces the Collective Aspects

In the literature, multiple accounts of autonomy have been put forward. To propose a working definition of autonomy for the purposes of this paper factoring in the interests of others and collective interests, we depart from the strictly individualistic understanding of autonomy and explore various approaches, including feminist, communitarian, public health, and environmental ethics, which situate the individual in relation to others, be it other individuals, the community, or the environment. We will refer to this as *collective autonomy*, to accommodate and account for the collective aspects of data processing alongside or in addition to the individual impacts. We find this appropriate because, akin to insights from the literature on the collective impact of data processing, individual choices in relation to, for instance, public health or the environment can result in collective effects beyond the immediate experience or control of an individual that are hard to ascribe to actions of that one individual or pertain to collective objectives.

To illustrate: "if a few parents refuse consent to their children's vaccination against a dangerous disease they risk little harm to their own or to others' children. But as more and more parents take this view, free riding fails and harm is risked to one's own and to others' children. Yet it is impossible to demonstrate that an individual parent who refuses vaccination thereby harms their own or others' children" (O'Neill, 2009: 45–46). Similar concerns arise in relation to environmental issues, where individual polluting action might create only a small level of pollution, which can then, when aggregated, result in large and long-term environmental harm (O'Neill, 2009: 45–46).

Further, such scholarship also recognizes the need to shift the focus away from individualized interventions, since these alone cannot fully respond to existing inequ(al)ities and address the determinants of health beyond an individual's direct control (see further Meier, 2007: 547, 553). Collective rights complement individual rights in achieving the same or a similar goal and act at a societal level ensuring public benefits that cannot be reached only through individual rights mechanisms (Meier, 2007: 551, 553). In this sense, parallels with data processing are evident, as such practices can produce not only individual harms or benefits, but also affect other individuals' and collective or societal interests beyond the control of an individual. Consequently, individualized responses that place "the individual in the position of the (collective) sovereign" to solve collective problems conflate the individual autonomy with collective self-rule, and thus conceal the right of the collective to also protect the common good and the autonomy of others affected from the individuals' behaviours (Bialasiewicz & Eckes, 2021), as discussed in the case of the pandemic (public health) responses. Accordingly, we conceive autonomy with this in mind.

It should also be stated that we do not aim to prescribe or delineate which interests specifically are to drive the decision-making in a data-driven, digital era. After all, thanks to technological progress, data processing practices are about collecting data about an "undefined number of people during an undefined period of time without a pre-established reason" (Van der Sloot in Reviglio & Alunge, 2020: 600), meaning that collectives are (re-)established continuously, ad hoc, and not in a fixed manner, "creating new means for identifying and grouping individuals" (Reviglio & Alunge, 2020: 600–1) virtually constantly. This makes identifying interests difficult, but also beyond the scope of the present paper. Instead, we submit that rather than only based on individualistic understanding, autonomy is also to be conceptualized and implemented with regard to the collective level that acknowledges the existence of varying interests and recognizes that data processing affects not only the individual (see Graef & van der Sloot, 2022). Our objective is to overcome the drawbacks of individualized responses present in existing and emerging legal frameworks, and to explore the possibility within existing legal frameworks to conceive and understand autonomy in this different, broader and more contextual manner.

2.2.1 From Individual to Collective Autonomy…

Several conceptions of autonomy are worth presenting here. First, etymologically, autonomy refers to the capacity for self-governance (Owens & Cribb, 2013: 264); in this regard, autonomy is conventionally conceptualized in the liberal thought tradition as individuals' right to be free from undue influences and interference by others in exercising their choices and satisfying their preferences independently and authentically (Dove et al., 2017: 152; Owens & Cribb, 2013: 264; Visagie et al., 2019). In democratic societies, this is usually expressed in fundamental rights instruments (Bialasiewicz & Eckes, 2021), with an insistence on individual responsibility (Lindbladh et al., 1998: 1018–1019). Such liberal view considers a person as self-contained, independent, and demarcated from the outside world, ensuring one lives peacefully with others (Parekh, 1992: 161, 163).

Second and by contrast, there are views that oppose the primacy of the individual and personal autonomy through individual rights and instead see autonomy as social in nature, which we consider more suitable to explore in context of collective effects of data processing. Relational approaches to autonomy were developed by considering "the influences of the myriad social structures in which a person is embedded" on one's capacities for autonomous deliberation and actual decisions (Mackenzie & Stoljar in Owens & Cribb, 2013: 265). It is not (simply) about shielding against the outside influence of others (see MacDonald, 2010: 203); autonomy is about effectively empowering individuals when interacting with each other (Nedelsky in MacDonald, 2010: 204). These views (Visagie et al., 2019: 171) thus acknowledge that individual decisions are shaped not only by individual reasoning, but also by ties to others and the material and social context of which one is part (Dove et al., 2017: 152; Spruit et al., 2016: 126; Gómez-Vírseda et al., 2019: 7; Milligan & Jones, 2016: 28). It is through these constraining or enabling (Owens & Cribb, 2013: 265–266; Wardrope, 2015) relationships, practices and intersubjective phenomena that autonomy emerges and develops (Nedelsky in Braudo-Bahat, 2017: 130; Chackal, 2017: 10–11). In this sense, 'practicing' autonomy refers to "constantly adapting

in relation to the ever-changing, surrounding context" (MacDonald, 2010: 203, referring to the concept of 'dynamic autonomy' by Keller).

Third, (Sub-Saharan) African conceptualization of personhood, Ubuntu, can be relied upon to elaborate such understanding further. To note, while we believe there are limits to importing non-Western philosophies like Ubuntu into the European context, we were nonetheless inspired by their insights and consider them relevant to our discussion. Ubuntu is inherently relational: the individual is inextricably linked to and owes her human nature to the community (see also below on communal conceptualizations of autonomy). Further, one becomes one's relational self through performing one's social duties and responsibilities to others, indicating that Ubuntu promotes a society in which everyone is expected to care for each other's needs (Mhlambi, 2020: 7; Reviglio & Alunge, 2020: 603–4). Relationality here refers to the acceptance of individuality of others: Ubuntu in this sense acknowledges that one is not complete in oneself, but relies on others — their community, environment, spirits — for completion. In the light of this, the individual is expected to use her liberty to act in harmony with the rest of society. Still, Ubuntu does not put forward "oppressive communalism" over an individual, but advocates for balancing and dialogue (Mhlambi, 2020: 13, 15–7).

As observed, while European philosophy conceives the self as something within oneself, in African thought it is seen as something outside, in relation to one's natural and social environment (Lassiter in Reviglio & Alunge, 2020: 604). In a way, autonomy then relates to thinking and acting for oneself (Code in Chackal, 2016: 125), one's own convictions, as well as to reflecting on these actions (Asveld, 2008: 248). Subsequently, the action dimension then allows us to think about autonomy in a more outward-facing way, namely to consider the effects and outcomes of decision-making and the ways in which these can be incorporated in a definition of autonomy. This inevitably brings to front the requirement for an understanding of autonomy that depends "upon an assessment of both the substantive *content* of the decision and the outcomes and opportunities to which the choice leads" (Owens & Cribb, 2013: 266). Taking this into consideration, 'acting for oneself' involves reflecting on the socio-political context in which one can or cannot act (Code in Chackal, 2016: 125). In this sense, the relational approach also acknowledges "the need to collectively organize society's resources so as to enable human flourishing" and "creating an environment in which each person is free to choose life options" (Zimmerman, 2017: 38–44), i.e. where said choices are properly supported (Wardrope, 2015: 51).

Fourth, Plumwood e.g. refers to the term 'ecological self' (in Chackal, 2016: 133) when considering a plurality of interests, as individuals indeed live with each other in interdependent ways. The term 'ecological self' "recognizes one's own interests, those of others, and when acting, acts out of consideration for others' interests and one's own". Autonomy can thus lie in the individual adjudicating between (her) competing interests (Chackal, 2016). Chackal here refers to ecological autonomy, which is comprised of an internal and external dimension. The former refers to thought, reflection, intelligence, cognition framing their perceptions and relations to the external, while the latter refers to action, environment, and other particularities that frame perception and social relationships. Both internal and external dimensions require competency and

authenticity (Chackal, 2017: 13–23), i.e. encompass "an internal epistemic capacity to think and an external actional capacity to act for oneself in relation to other individuals and environments", thus sustaining and facilitating autonomy (Chackal, 2018) in the sense of relational interdependency (Chackal, 2016).

Lastly, there is scholarship that (similarly) develops a more collective or communal conceptualization of autonomy that stresses interdependence and collaboration in decision-making based on shared beliefs (Visagie et al., 2019: 169).[1] It rests upon common good considerations, common practice of trust (Ramabu, 2019: 187),[2] and acting in solidarity with others and identifying with them (Metz & Gaie in Visagie et al., 2019: 171; Gómez-Vírseda et al., 2019: 7; Dove et al., 2017: 152).Similarly, the concept of community autonomy emerges "when individuals express a willingness to collectivize for a given purpose and determine a way to aggregate their individual choices into collective ones toward that end" (Chackal, 2016: 132), whereby the focus is on the group, which "includes but is not deducible to the individuals within it" (ibid.). Such collective action requires shared knowledge and commitment in determining the community interests and the ways to achieve them (Chackal, 2016).

While the concept of this more collective or communal autonomy usually refers to a group, "the justification of legal and moral requirements, as well as the foundations of justice" (Reis-Dennis, 2020: 10), so (also) collective or societal interests, can also take place within respect for autonomy that pertains to an individual herself. Namely, Reis-Dennis (2020) maintains that insistence on the right of non-interference and self-determination is not suitable to address the communal matters of, in his case, public health, and proposes a 'thick' understanding of autonomy, which requires that "we bring our behavior into line with rules and laws that reflect a commitment to equality and respect" of others (Reis-Dennis, 2020: 6). As a result of this, the principle of autonomy generates rules not because everyone does what they want but because it is a right to make decisions that affect one's life in accordance with rationally acceptable principles (Reis-Dennis, 2020: 5–6 and 9–10).

This discussion is important as it challenges an understanding of (individual) autonomy, which "if unconditioned by competing principles (beneficence, justice, non-maleficence) would give competent adults the right to do anything they desired to do so long as they satisfied certain baseline psychological conditions" (Reis-Dennis, 2020: 2). The unchallenged understanding would indeed support the view that "autonomy is suitable for individual interactions, but must be overridden in the name of beneficence when public health is at stake", indicating a consequentialist approach (Reis-Dennis, 2020: 7). What Reis-Dennis (2020: 7–8) submits instead is that acts such as mandated isolation and quarantine, in cases where individual and collective interests are at stake, should not be understood as a limitation of autonomy or its subordination to other ethical principles, but rather as its *expression* rooted in rules that reflect one's concern for autonomy and dignity of their fellow citizens. In this perspective, respect for autonomy does two things: it not only rejects

[1] These authors advocate for an integrated informed consent approach based on Afro-communitarianism.

[2] Ramabu discusses the notion of 'community consent' and ways in which human beings should relate to the well-being of society, based on collective agency and consenting process in Botswana communities.

paternalism in, e.g. promoting welfare, it also generates positive rules of conduct that we could rationally endorse and does not allow acts that would violate others' status as equal moral agents (Reis-Dennis, 2020: 7–10), bringing the concept in the collective realm. Such an understanding can give us "powerful theoretical resources we might use to consider the justification of legal and moral requirements, as well as the foundations of justice" (Reis-Dennis, 2020: 7–10). What this could also point to is that when collective interests are at stake, a more collective understanding of autonomy is possible only when a consensus and a clear guidance exists regarding the shared values, principles, and rules so that such an understanding of autonomy in fact results in its expression rather than subordination.

2.2.2 ... To Propose a Twofold Definition of Autonomy

After surveying these various theoretical approaches to conceiving autonomy that would encompass both individual and collective interests, we synthesize them in order to develop a working definition of autonomy to use in the remainder of the paper. Such a definition is inherently multi-dimensional as it points to different dimensions (i.e. interests) that the above-discussed accounts focus on and the trade-offs they prioritize (see Wittrock, 2022); against this, we later assess the regulatory instruments and the way in which they approach the balancing of these multiple interests.

Our proposal to define autonomy is, in line with e.g. Chackal's (see above), equally inward- (thought) and outward-looking (action). In the inward-looking sense, autonomy covers the capacity for individual reasoning and freedom from interference, and the consideration of (outcomes of) choices in view of one's own interests. In the outward-looking sense, autonomy refers to relationships, conditions, and context of one's choice that can facilitate autonomy or not (Laitinen & Sahlgren, 2021) and, arguably, the factoring of consequences for other individuals' and collective interests. Beyond that, collective interests can be used to formulate and operationalize the requirements of equality and respect for oneself and for others.

It is worth mentioning that beyond this twofold definition of autonomy that looks at the inward (own interests) as well as the outward dimension (how one's interests relate to other individuals' and collective interests), a completely different understanding of autonomy and human condition in the data-driven, digital era is possible (see, e.g., Floridi, 2015), which puts the emphasis on the collective as such instead of on the individual (see, e.g., Krause, 2015; Bollier & Helfrich, 2019; van Roermund, 2020; Staal, 2020). However, our paper maintains the vision of autonomy that can integrate and balance the different dimensions because this reflects current regulatory approaches. A limitation of our analysis is therefore that it does not allow for disregarding individual interests altogether and for solely framing issues as collective problems. Our objective is not to discuss what the optimal form or interpretation of autonomy is, but to explore to what extent the concept of autonomy underlying current regulation can reflect the societal reality in data markets that is inherently characterized by relational and collective dimensions in addition to individualistic aspects.

3 Autonomy and Data Processing: Perspectives from Regulation

In this section, we will assess the three legislative initiatives regulating data mentioned in the introduction (Digital Markets Act, Data Act and GDPR) by reference to the conceptual discussions relating to autonomy outlined above. To identify to what extent the regulatory initiatives reflect the multi-dimensional nature of autonomy, we will analyse three aspects, namely: (1) the extent of control and responsibility an individual has over the protection of her personal data (the inward-looking dimension of autonomy); (2) the limits that other individuals' and collective interests pose to the exercise of control and responsibility by an individual (the outward-looking dimension of autonomy); and (3) if relevant, how such balancing of interests takes place and by whom. This will allow us to explore how regulatory initiatives can be brought in line with insights from literature.

We believe it is fundamental for the legislator to make the balancing between the different interests explicit when drafting data regulations in order not to overlook one of the dimensions of autonomy. Yet, we will see that the legislator tends not to think about these two dimensions when legislating, and rather solely focuses (unconsciously) on one of these dimensions. We argue that this is notably the case in the Digital Markets Act and in the Data Act proposal. On the contrary, the GDPR seems to stand out a bit in this regard, as some of its provisions point to the necessity to find a balance between the interests of the individual and those of other individuals' and collective interests. This is notably visible from the way in which the data portability right has been designed (GDPR: Art. 20), which we will analyse below. However, while the GDPR makes room for such trade-offs, we will argue that it does not go far enough in considering collective interests.

3.1 Regulation of Personal Data Combination in the Digital Markets Act

The Digital Markets Act (DMA) aims to complement the EU competition rules by imposing additional ex ante obligations on gatekeepers (powerful providers that meet certain criteria (DMA: Art. 3(1) and (2))) that offer so-called core platform services ("CPS") (e.g. online search engines, online social networking services, advertising services (DMA: Art. 2(2))). As one of these obligations, Article 5(2) DMA obliges a gatekeeper to refrain from combining personal data sourced from its CPS with personal data from any other services offered by the gatekeeper or with personal data from third-party services, unless the user has provided consent in the meaning of the GDPR. While the choice to let users decide on whether a gatekeeper can combine personal data is welcome from the perspective of the inward-looking dimension of autonomy,[3] it does not leave any room for considering how such a decision of an individual can affect the other individuals' and collective interests in contestable markets.

The combination of personal data across services can allow for the provision of more relevant and personalized services to the benefit of the individual interested in

[3] Although one may wonder if individuals are capable of making such decisions, in particular against the background of the use of nudging and dark patterns by market players (Podszun, 2021: 6–7).

receiving such services. However, because data is relational, other individuals may be affected too without having had any say in the decision to combine data of someone they relate to or with whom they share common characteristics. And at the same time, markets will arguably become less contestable, harming the collective interest in competitive markets because the extent of personal data combination by gatekeepers increases, allowing them to enter an expanding number of related markets to the detriment of smaller rivals who do not have the same reach and control over markets (Condorelli & Padilla, 2020).

As a result, Article 5(2) DMA gives the individual full control over the combination of her personal data but does not impose any limits to protect other individuals' and collective interests. In other words, there is no attention for the outward-looking dimension of autonomy. This is remarkable as it may impact the extent to which the DMA will reach its objective of creating fair and contestable digital markets (DMA: Art. 1(1)). If the combination of personal data is considered a practice that can limit the contestability of markets, the extent to which Article 5(2) DMA will contribute to the creation of contestable markets is now left in the hands of individual users. The more individuals consent to their personal data being combined by a gatekeeper; the less contestable digital markets may become.

As such, Article 5(2) of the DMA overlooks the relational and collective nature of data processing and does not allow for any balancing. To provide more room for considering the interests of others and collective interests, the provision could have referred to the performance of a contract (GDPR: Art. 6(1)(b)) instead of consent as a ground for combining personal data across services (Graef, 2021). Relying on the performance of a contract would have allowed gatekeepers to combine personal data only to the extent necessary for delivering a service in compliance with the contract as entered into by a user (EDPB Guidelines 2/2019). This could arguably have allowed for a balancing between the interests of the individual, the interests of others and collective interests.

If it is not possible to deliver a service without combining personal data, the merging of data should be possible. In such circumstances, the combination of personal data can bring value to individuals who have asked for the service and to the collective interest in the form of new services for which demand exists. An example could be a new application, bringing together personal data from a gatekeeper's email service and map service, to advise a user on how to best organize her travel movements (Graef, 2021). Individuals would still hold control over their personal data in line with the inward-looking dimension of autonomy, because they can choose whether or not to receive that service or application from a gatekeeper. Due to the fact that only the combination of personal data strictly necessary to perform the contract is allowed, disproportionate effects on the interests of others and collective interests would have been restricted in line with the outward-looking dimension of autonomy.

Even though the assessment will still predominantly focus on what is reasonable or fair in the relationship of the data controller with the individual, relying on the performance of a contract opens up more possibilities to consider the interests of others and the collective interest than relying on consent. By relieving individuals of the responsibility to decide on their own whether personal data should be combined

across services, it would thus have been possible to better reflect the relational and collective impact of data processing into the DMA. Even though it is a valid policy choice to give precedence to the control by individuals as an end-result, it is at least peculiar that this happened as part of a legislative instrument with the aim of protecting contestable and fair markets in the collective interest, without any possibility to balance the inward- and outward-looking dimensions of autonomy.

3.2 Data Act's Exclusion of Gatekeepers as Beneficiaries of Data Access

At the other end of the spectrum are situations where collective interests are pursued without any regard for individual interests. The Data Act proposal's (DA) exclusion of gatekeepers as beneficiaries of data access is an example of this. In this proposal, the Commission provides users (individuals as well as businesses) with a right to access data generated by the use of products or related services (DA: Art. 4(1)) and with a right to share that data with third parties (DA: Art. 5(1)). These rights focus in particular on the 'Internet of Things' (IoT), where manufacturers have been able to limit the access and exchange of data through technical restrictions in the design of their products and services. The DA data access right lets users obtain the data that is necessary to benefit from repair and other services offered by other providers beyond the manufacturer of the IoT device and thereby also stimulates businesses in launching innovative and more efficient services (DA: recital 19). However, the data access right of users under the DA does have an important limit.

Article 5(2) of the DA namely provides that an undertaking qualifying as a gatekeeper under the DMA is not eligible as a third party to receive data generated by the use of a product or related service from a user or from a data holder upon the request of a user. And according to Article 6(2)(d) of the DA, other third parties cannot make available any data they receive to a gatekeeper either. Recital 36 of the DA explains that "given the unrivalled ability of these companies to acquire data, it would not be necessary to achieve the objective of this Regulation, and would thus be disproportionate in relation to data holders made subject to such obligations, to include such gatekeeper undertakings as beneficiaries of the data access right".

It thus seems that the Commission has decided to focus on the collective interest of avoiding further data concentration in the hands of gatekeepers and the interests of other individuals in limiting the amount of knowledge about them that is made available to gatekeepers via their contacts. The result is that the interest of individuals to control to whom they can port their data generated by the use of a product or related service is restricted. Users cannot move their data that they obtain from a data holder through the DA to a gatekeeper, which limits their freedom of choice. For instance, users of the virtual assistants provided by Google and Amazon cannot use the Data Act to integrate data from smart fridges or other devices into their smart home systems. This may deprive consumers of the benefits of integrating devices from different manufacturers into the most commonly used smart home systems at the moment (Martens, 2023: 15–16). As a result, the DA's exclusion of gatekeepers as beneficiaries of data access focuses solely on the outward-looking dimension of autonomy without allowing for any balancing with the inward-looking

dimension of autonomy. Within the DA, there is no room for users to bring their data to a gatekeeper. This extent of control is taken away from users.

One can criticize that individuals do not have any possibility to let their data flow to gatekeepers under the DA, thereby disregarding the inward-looking dimension of autonomy. Engaging in a trade-off between the two dimensions of autonomy could have led to a more nuanced approach, for instance by requiring gatekeepers to keep the data they obtain from users or third parties under the DA separate from the data they already have at their disposal from their activities in other areas. This would give users leeway to bring their data to gatekeepers if they choose to do so, while providing some safeguards to protect the collective interest in not letting the control of gatekeepers over data expand further and the interests of others in ensuring that gatekeepers do not know even more about them through data shared by their contacts. At the same time, experience with the enforcement of the GDPR's principle of purpose limitation indicates that it is tricky to monitor and ensure that data is not used for more than one purpose inside a company (Brave, 2020). For this reason, the exclusion of gatekeepers as beneficiaries of data access under the proposed DA may be a far-reaching but proportionate measure to effectively protect the collective interest and the interests of others. While this could be seen as a welcome step in acknowledging the outward-looking dimension of autonomy, it is not clear whether this results from a conscious choice on the part of the legislator to disregard the individual interest in order to serve the collective interest and the interests of others. More clarity on whether and how the legislator indeed conducted such a balancing, for instance in the recitals, would have been welcome to guide the interpretation and implementation of the provision.

3.3 GDPR's Right to Data Portability

The above-mentioned aspects of the DMA and the DA present the two extreme ends on the spectrum, where no room is foreseen to balance the inward- and outward-looking dimensions of autonomy in the implementation of the respective legal obligations. In case of the discussed provisions of the DMA and the DA, the legislator solely focuses on one of these dimensions of autonomy. To be more precise, we believe that the objectives pursued and the design choices of the provisions at hand implicate that only one dimension of autonomy is considered, even though the legislator may actually not explicitly have made a conscious choice about only opting for that single dimension. There may be good reasons for the legislator to do so, although care should be taken to ensure that the legislation reflects the reality on the market as well as the policy objective of the legislative instrument.

On the contrary, the GDPR seems to acknowledge the necessity to find a balance between the interests of the individual who takes a decision about her personal data, and those of other individuals' and collective interests. Interestingly, it does not attempt to settle this trade-off once and for all, by making an explicit choice to prioritize either the inward- or outward-looking dimension of autonomy. Rather, the GDPR invites to conduct this balancing at the stage of interpretation and implementation of some of its obligations. The right to data portability (GDPR: Art. 20) provides an example of such a scenario.

The GDPR introduced a right to data portability, which enables an individual to transfer personal data to another controller and thereby increases the control of individuals over their data. For instance, an individual could decide to port all of her pictures from one social media to another, or her favourite songs' playlist from one streaming app to another. An important characteristic of the right to portability is that it only pertains to "personal data concerning [the individual]" (GDPR: Art. 20(1)), which illustrates the individual-centric focus of this right.

At first glance, this could be seen as overlooking the relational and collective nature of data. In fact, the Article 29 Working Party (2017: 9) — today the European Data Protection Board — seems to be wary of this potential gap without however explicitly mentioning or recognizing it, as it outlined that the expression "personal data concerning [the individual]" should not be interpreted too strictly by limiting the scope of the data portability right to personal data "exclusively" pertaining to the individual. For example, reference is made to the case of telephone records or other interpersonal messaging systems that may include information about third parties with whom the data subject has been in contact.

Yet, Article 20(4) of the GDPR also provides that the right to data portability should not adversely affect the rights and freedoms of others. As such, the GDPR's right to data portability arguably considers both the inward- and outward-looking dimensions of autonomy, as it makes room for considering other individuals' interests.

The balancing between these inward- and outward-looking dimensions of autonomy will need to be done on a case-by-case basis by the individual requesting the porting and the data controllers involved (i.e. the original controller and the recipient controller). While the GDPR itself does not further clarify how such balancing should be tackled, the Article 29 Working Party (2017) has published guidelines on how to conduct the balancing with the rights and interests of others.

For instance, porting a picture from one social network to another might be problematic if other people are tagged on the picture, as their right to personal data protection might be adversely affected by the transfer. According to the Article 29 Working Party (2017:11), such an "adverse effect" would occur if the sharing would prevent these other individuals "from exercising their rights as data subjects under the GDPR (such as the rights to information, access, etc.)". In order to avoid these "adverse effects", the Article 29 Working Party (2017:12) suggests that the processing of these other individuals' personal data should be authorized only insofar as these data remain under the sole control of the individual at the origin of the sharing, and that they should only be processed for the purposes determined by this individual. It also invites both the data holder and the recipient to implement technical tools allowing the individual to select the personal data she wishes to share, while excluding, where possible, the personal data of other individuals. For instance, software could be developed to separate automatically the pictures where several individuals are present from landscape pictures and the pictures where only the individual making the portability request is visible. Indeed, the "adverse effects" of portability on the right of others would only need to be considered for the first category, while the two other categories could be ported without hindrance.

While such guidance is welcome, it still leaves room for data controllers to act in their own commercial interests by limiting the extent of data portability on the ground that it would (arguably) "adversely affect" other individuals (Egan, 2019; Martinelli, 2019). Indeed, an expansive interpretation of the scope of the right to data portability may not be to the benefit of data controllers as it diminishes their control over individuals who are now free to transfer their data to other services. Effective monitoring by data protection authorities is necessary to ensure that the implementation of the right to data portability reflects a balance between the interests of the individual and the interests of others, and is not dominated by the commercial interests of the data controller, which can be tempted to disguise anti-competitive practices as (alleged) data protection concerns (Geradin et al., 2020).

Importantly however, although the GDPR's right to data portability explicitly provides room for considering the interests of others, it somewhat overlooks collective interests. Yet, beyond its objective of empowering individuals to control their personal data, the GDPR's right to data portability was at the time of its adoption also argued to be capable of encouraging competition in data markets (Council, 2016: 89) by reducing user lock-in. However, this more collective interest is not visible in the text of Article 20 GDPR that regulates the relationship between a data controller and a data subject with some consideration for the impact on the rights and freedoms of other individuals. In fact, the Article 29 Working Party (2017: 4) guidelines on Article 20 GDPR even explicitly state that the main objective of this right is to promote "data subject empowerment" and that the GDPR aims to regulate the processing of personal data, and not to deal with competition issues, which seems to further exclude the consideration of the collective interest in encouraging competition in data markets.

One way of integrating the collective interest of competitive or innovative data markets into the GDPR's right to data portability could be to tailor the interpretation of its requirements to the market position of the data controller at stake. For instance, powerful data controllers can be expected to have more resources and expertise available to create particularly effective forms of data portability that allow for continuous and real-time exchanges of data (Krämer et al., 2020: 79–83). Such a stricter interpretation of the requirements of the GDPR's right to data portability would not only stimulate the collective interest in competitive and innovative data markets where powerful data controllers can now dictate the extent of data portability, but also increase the control of individuals vis-à-vis such powerful data controllers on whom they are dependent to receive certain services.

In fact, one could argue that this more tailored approach has been included in the DMA, which provides for stricter data portability conditions for powerful data controllers qualifying as gatekeepers. This is because Article 6(9) of the DMA now explicitly requires gatekeepers to facilitate continuous and real-time portability building on the GDPR. As such, this provision of the DMA can be said to integrate the collective interest into the issue of data portability, even though the GDPR's right to data portability does not explicitly provide for this. This also shows how legislative instruments can complement each other in covering different dimensions of autonomy. In this regard, it is also worth pointing out that although the GDPR's right to data portability overlaps to some extent with the data access right

of users under the proposed Data Act in terms of the scope of data covered (Tombal & Graef, 2023: 6–16), Article 20 GDPR, unlike the proposed Data Act, does not impose restrictions on who can receive ported personal data and thus also allows individuals to transfer personal data to gatekeepers.

Even though this analysis shows that the different dimensions of autonomy can be found in legislative instruments, consideration for the collective impacts of data processing so far seems to be the result of mere chance rather than an explicit awareness on the part of the legislator. To bridge the gap between theory and practice, the collective effects of data processing — already well-recognized in literature for years — deserve to feature more prominently in regulatory discussions as well. This would not only make the relevant trade-offs visible, but also allow a democratically elected legislator to conduct the balancing exercise instead of leaving this important task up to private parties.

4 Conclusion

To conceptualize the notion of autonomy in the context of the relational and collective impact of data processing already recognized in literature, we relied on an understanding of autonomy that moves away from a purely individualistic conception and integrates relational and collective dimensions by taking into account its inward- and outward-looking dimensions. While the inward-looking dimension focuses on the ability of an individual to make free and independent decisions in her own interests, the outward-looking dimension considers the relationship of one's choices with other individuals' and collective interests. This twofold definition of autonomy acknowledges that divergent autonomies can interfere and that not everyone's (individual) autonomy can be optimized at the same time. This thus requires balancing the interests of the individual who takes a decision about her personal data, with other individuals' and collective interests.

Building on this working definition of autonomy, we assessed three legislative instruments regulating data to identify to what extent the multi-dimensional nature of autonomy drawn from theory is or can be reflected in practice in interpreting and implementing key data-related obligations. Concretely, we examined how to make trade-offs between different interests explicit and thereby bring the regulation of data markets more in line with the current societal reality that is increasingly dominated by relational and collective effects of data processing. Our main finding in this regard is that the trade-offs between the individual interest, the interests of others and the collective interest are sometimes overlooked by the legislator in the regulatory frameworks.

This is evidenced by the DMA's choice to leave the extent of personal data combination completely in the hands of individual users' consent, and by the DA's opposite choice to focus on the interests of others and the collective interest while overlooking the individual's ability to control the use of her personal data by excluding gatekeepers as beneficiaries of the IoT data access right. Other areas, such as the GDPR's right to data portability, already partly acknowledge the need to balance the different interests and dimensions of autonomy, as Article 20(4) GDPR provides

that the individual's interests must be balanced with other individuals' interests. However, the GDPR leaves a lot of discretion to market players with the risk that they act in their own commercial interests without adequately reflecting the interests of others. Moreover, although it explicitly provides room for considering the interests of others, the GDPR portability right overlooks collective interests. As such, our analysis shows that legislators still need to become more aware of the different interests in order to make the trade-offs explicit and to ensure that the relevant obligations are implemented accordingly.

Although the paper has only explored a selected number of horizontal regimes relevant to the regulation of data, our insights have a broader relevance for ongoing and future initiatives in the area. In the context of the European Data Strategy, the European Commission is for instance planning to facilitate the establishment of so-called 'common European data spaces' in specific sectors of particular importance to stimulate data-driven innovation (European Commission, 2020: 12). The design of these data spaces, among other things, also requires balancing individual and collective interests by opening up more data for use in the economy and society, while letting individuals and business retain some level of control. The proposal for a Regulation for a European Health Data Space, which is the first of the nine envisioned common data spaces, offers an illustration of how this balancing is done in the context of opening up health data (Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, 2022a, b). On the one hand, the proposed European Health Data Space aims to empower individuals to have more control over their health data when it comes to the delivery of healthcare. On the other hand, it facilitates health data sharing for secondary use, that is for research, innovation, and policy-making purposes contributing to the general interest of society "at the cost of self-determination of the individual" (Slokenberga, 2022: 135), as its general approach is not to rely on consent of the data subject for data reuses (Shabani & Yilmaz, 2022: 132). Further, the proposal requires data holders to make certain categories of health data available for secondary use, access to which is granted through a permit-based system. This demonstrates the relevance of balancing individual control against other, societal considerations[4] within the European Health Data Space as another legislative area beyond the ones studied in this paper.

In order to trade-off the respective considerations and find the right outcome for different settings, consensus is first required on what exactly collective interests should entail when it comes to data processing. This will require setting up common principles upon which such balancing and dialogue can take place, and ensuring consistency in approaches across regulatory frameworks. While the considerations involved in the balancing exercise are similar, different circumstances and policy objectives will call for different outcomes. Our paper hopes to have provided a starting point for such a discussion and contribute to bridging the gap between the theoretical discussions in literature and the practice of regulating data processing so far.

[4] Whether the actual balance between the interests at hand established in the European Health Data Space is indeed appropriate for the characteristics and sensitivity of the sector, and whether the 'general interest of society' is adequately defined, is however a subject of debate that is beyond the scope of this paper (see, e.g., Shabani and Yilmaz, 2022; Slokenberga, 2022, discussing the protection of the data subject; and Petrocnik, 2022: 127, proposing to include in the discussions on the governance of health data sharing also how to share the value stemming from its use, to ensure the European Health Data Space will truly "work for people and science").

Acknowledgements The authors would like to thank the anonymous reviewers and the participants to the "Data and the Common – Infoleg Workshop" for their useful comments on earlier drafts, in particular Prof. Dr. Nadya Purtova, Dr. Gijs van Maanen and Dr. Katja de Vries.

Author Contribution All authors contributed equally.

Funding This work was undertaken in the context of the Digital Legal Studies research initiative, which is funded through the Law Sector Plan of the Dutch Ministry of Education, Culture and Science (OCW).

Data Availability No data was generated or analysed in the context of this article.

Declarations

Conflict of Interest The authors declare no competing interests.

References

(Proposed) Legislation

Regulation (EU). (2022a). 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), 12 October 2022, OJ L265/1.

Regulation (EU). (2022b). 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act), 3 June 2022, OJ L152/1.

Regulation (EU). (2016). 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), 4 May 2016, OJ L119/1.

Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), 23 February 2022, COM (2022a) 68 final.

Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space, 3 May 2022, COM (2022b) 197 final.

Secondary sources

Acemoğlu, D., Makhdoumi, A., Malekian, A., & Ozdaglar, A. (2019). Too much data: Prices and inefficiencies in data markets. *NBER Working Papers 26296*. https://ideas.repec.org/p/nbr/nberwo/26296.html

Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. *Sloan Foundation Economics Research Paper No. 2580411*. https://ssrn.com/abstract=2580411

Article 29 Working Party. (2017). Guidelines on the right to data portability, WP 242 rev.01, 13 April 2017.

Asveld, L. (2008). Mass vaccination programmes and the value of respect for autonomy. *Bioethics, 22*(5), 245–257.

Ben-Shahar, O. (2019). Data pollution. *Journal of Legal Analysis, 11*, 104–159.

Bialasiewicz, L., & Eckes, C. (2021). Individual sovereignty' in pandemic times – A contradiction in terms. *Political Geography, 85*. https://doi.org/10.1016/j.polgeo.2020.102277

Bietti, E. (2020). Consent as a free pass: Platform power and the limits of the informational turn. *Pace Law Review, 40*, 310–398.

Bollier, D., & Helfrich, S. (2019). *Free, fair and alive*. New Society Publishers.

Braudo-Bahat, Y. (2017). Towards a relational conceptualization of the right to personal autonomy. American University Journal of Gender, Social Policy & the Law, 25(2), 111-154

Brave. (2020, February 12). *Response to consultation regarding online platforms and digital advertising*. Retrieved August 17, 2022, from https://brave.com/wp-content/uploads/2020/02/12-February-2020-Brave-response-to-CMA.pdf

Calo, R. (2014). Digital market manipulation. *George Washington Law Review, 82*(4), 995–1051.

Chackal, T. (2016). Autonomy and the politics of food choice: From individuals to communities. *Journal of Agricultural Environmental Ethics, 29*, 123–140.

Chackal, T. (2017). The internal and external dimensions of ecological autonomy. *Dissertation Submitted to the Graduate School in Partial Fulfillment of the Requirements for the Degree Doctor of Philosophy*. https://getd.libs.uga.edu/pdfs/chackal_anthony_e_201712_phd.pdf

Chackal, T. (2018). Place, community, and the generation of ecological autonomy. *Environmental Ethics, 40*(3), 215–239.

Chang, A. (2018, May 2). *The Facebook and Cambridge Analytica scandal, explained with a simple diagram*". Vox. Retrieved August 17, 2022, from https://www.vox.com/policy-and-politics/2018/3/23/17151916/facebook-cambridge-analytica-trump-diagram

Condorelli, D., & Padilla, J. (2020). Harnessing platform envelopment in the digital world. *Journal of Competition Law & Economics, 16*(2), 143–187.

Council. (2016). Position (EU) No 6/2016 of the Council at first reading with a view to the adoption of a Regulation of the European Parliament and of the Council 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), Brussels, 3 May 2016, OJ C 159/1.

De Brouwer, S. (2020). Privacy self-management and the issue of privacy externalities: Of thwarted expectations, and harmful exploitation. *Internet Policy Review, 9*(1), 1–29.

Delacroix, S., & Veale, M. (2020). Smart technologies and our sense of self: Going beyond epistemic counter-profiling. In M. Hildebrandt & K. O'Hara (Eds.). *Life and the Law in the Era of Data-Driven Agency* (pp. 80–99). Edward Elgar Publishing. https://doi.org/10.4337/9781788972000

Dencik, L., Jansen, F., & Metcalfe, P. (2018). A conceptual framework for approaching social justice in an age of datafication. *Working Paper*. https://datajusticeproject.net/wp-content/uploads/sites/30/2018/11/wp-conceptual-framework-datajustice.pdf

Dove, E. et al. (2017). Beyond individualism: Is there a place for relational autonomy in clinical practice and research. *Clinical Ethics, 12*(3), 150–165.

Dworkin, G. (1988). *The theory and practice of autonomy*. Cambridge University Press.

Egan, E. (2019). Data Portability and Privacy: Charting a way forward. *Facebook White Paper*. https://about.fb.com/wp-content/uploads/2020/02/data-portability-privacy-white-paper.pdf

European Commission. (2020). Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions "A European strategy for data", Brussels, 19 February 2020, COM(2020) 66.

European Data Protection Board. (2019). Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects. 9 April 2019.

Fairfield, J. A., & Engel, C. (2015). Privacy as a public good. *Duke Law Journal, 65*(3), 385–457.

Floridi, L. (2015). The Onlife Manifesto. Being human in a hyperconnected era. Springer.

Geradin, D., Karanikioti, T., & Katsifis, D. (2020). GDPR myopia: How a well-intended regulation ended up Favoring Google in Ad Tech. *TILEC Discussion Paper DP 2020–012*. https://ssrn.com/abstract=3598130

Graef, I. (2021, September 2). *Why end-user consent cannot keep markets contestable: A suggestion for strengthening the limits on personal data combination in the proposed digital markets*. Verfassungsblog. Retrieved August 17, 2022, from https://verfassungsblog.de/power-dsa-dma-08/

Graef, I., & Van der Sloot, B. (2022). Collective data harms at the crossroads of data protection and competition law: Moving beyond individual empowerment. *European Business Law Review, 33*(4), 513–536.

Granville, K. (2018, March 19). *Facebook and Cambridge Analytica: What you need to know as fallout widens*. New York Times. Retrieved August 17, 2022, from https://www.nytimes.com/2018/03/19/technology/facebook-cambridge-analytica-explained.html

Gómez-Vírseda, C., de Maeseneer, Y., & Gastmans, C. (2019). Relational autonomy: What does it mean and how is it used in end-of-life care? A systematic review of argument-based ethics literature. *BMC Medical Ethics, 20(76)*. https://doi.org/10.1186/s12910-019-0417-3

Hallinan, D., Friedewald, M., & De Hert, P. (2013). Genetic data and the data protection regulation: Anonymity, multiple subjects, sensitivity and a prohibitionary logic regarding genetic data? *Computer Law & Security Review, 29*(4), 317–329.

Hess, C., & Ostrom E. (2007). Introduction: An overview of the knowledge commons. In C. Hess & E. Ostrom (Eds.) *Understanding Knowledge as Commons: From Theory to Practice*. MIT Press.

Hildebrandt, M. (2015). *Smart Technologies and the End(s) of Law*. Edward Elgar.

Krämer, J., Senellart, P., & De Streel, A. (2020). Making data portability more effective for the digital economy. *CERRE report.* https://cerre.eu/publications/report-making-data-portability-more-effective-digital-economy/

Krause, S. (2015). *Freedom beyond sovereignty*. University of Chicago Press.

Laitinen, A., & Sahlgren, O. (2021). AI systems and respect for human autonomy. *Frontiers in Artificial Intelligence.* https://doi.org/10.3389/frai.2021.705164

Lindbladh, E., et al. (1998). Equity is out of fashion? An essay on autonomy and health policy in the individualized society. *Social Science & Medicine, 46*(8), 1017–1025.

MacCarthy, M. (2011). New directions in privacy: Disclosure, unfairness and externalities. *Journal of Law and Policy for the Information Society, 6*, 425–512.

MacDonald, F. (2010). Relational group autonomy: Ethics of care and the multiculturalism paradigm. *Phypatia, 25*(1), 196–212.

Mantelero, A. (2016). Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. *Computer Law & Security Review, 32*(2), 238–255.

Martens, B. (2023). Pro- and anti-competitive provisions in the proposed European Union Data Act. *Bruegel Working Paper 01/2023*. https://www.bruegel.org/sites/default/files/2023-01/WP%2001.pdf

Martinelli, S. (2019). Sharing data and privacy in the platform economy: The right to data portability and "porting rights." In L. Reins (Ed.), *Regulating New Technologies in Uncertain Times* (pp. 133–152). T.M.C. Asser Press.

Meier, B. (2007). Advancing health rights in globalized world: Responding to globalization through collective human right to public health. *Journal of Law, Medicine and Ethics, 35*(4), 545–555.

Mhlambi, S. (2020). From rationality to relationality: Ubuntu as an ethical & human rights framework for artificial intelligence governance. *Carr Center Discussion Paper Series, 2020–009*. https://carrcenter.hks.harvard.edu/publications/rationality-relationality-ubuntu-ethical-and-human-rights-framework-artificial

Milligan, E., & Jones, J. (2016). Rethinking autonomy and consent in healthcare ethics. In P. A. Clark (Ed.), *Bioethics - Medical, Ethical and Legal Perspectives* (pp. 21–38). IntechOpen.

O'Neill, O. (2009). *Autonomy and trust in bioethics*. Cambridge University Press.

Owens, J., & Cribb, A. (2013). Beyond choice and individualism: Understanding autonomy for public health ethics. *Public Health Ethics, 6*(3), 262–271.

Parekh, B. (1992). The cultural particularity of liberal democracy. *Political Studies, 40*(1), 160–175.

Petrocnik, T. (2022). Health data between improving health(care) and fuelling the data economy: Editorial. *Technology and Regulation, 2022,* 124–127. https://doi.org/10.26116/techreg.2022.012

Reviglio, U., & Alunge, R. (2020). "I am datafied because we are datafied": An Ubuntu perspective on (relational) privacy. *Philosophy & Technology, 33*, 595–612.

Rouvroy, A. (2016). "Of data and men": Fundamental rights and liberties in a world of big data. *Report for the Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (T-PD)*, T-PD-BUR(2015)09REV.

Rouvroy, A. (2018). Homo juridicus est-il soluble dans les données ? In E. Degrave, C. de Terwangne, S. Dusollier, & R. Queck (Eds.), *Law, Norms and Freedoms in Cyberspace / Droit, normes et libertés dans le cybermonde: Liber Amicorum Yves Poullet* (pp. 417–444). Larcier.

Rouvroy, A., & Berns, T. (2013). Gouvernementalité algorithmique et perspectives d'émancipation. Le disparate comme condition d'individuation par la relation ?. *Réseaux*, *177(1),* 163–196.

Rouvroy, A., & Poullet, Y. (2009). The right to informational self-determination and the value of self-development: Reassessing the importance of privacy for democracy. In S. Gutwirth, Y. Poullet, P. de Hert, C. de Terwangne, & S. Nouwt (Eds.), *Reinventing data protection: Proceedings of the International Conference (Brussels, 12–13 October 2007)* (pp. 45–76). Springer.

Podszun, R. (2021). Should gatekeepers be allowed to combine data? Ideas for Art. 5(a) of the draft Digital Markets Act. *SSRN Working Paper June 2021*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3860030

Ramabu, N. M. (2019). Whose autonomy is it? Botswana socio-ethical approach to the consenting process. *Developing World Bioethics*. https://doi.org/10.1111/dewb.12253

Reis-Dennis, S. (2020). Understanding autonomy: An urgent intervention. *Journal of Law and the Biosciences, 7(1)*. https://doi.org/10.1093/jlb/lsaa037

Rodwin, M. A. (2010). Patient data: Property, privacy & the public interest. *American Journal of Law & Medicine, 36*(4), 586–618.

Shabani, M., & Yilmaz, S. . (2022). Lawfulness in secondary use of health data: Interplay between three regulatory frameworks of GDPR, DGA & EHDS. *Technology and Regulation*, 2022, 128–134. https://doi.org/10.26116/techreg.2022.013

Slokenberga, S. (2022). Scientific research regime 2.0? Transformations of the research regime and the protection of the data subject that the proposed EHDS regulation promises to bring along. *Technology and Regulation*, 2022, 135–147. https://doi.org/10.26116/techreg.2022.014

Smuha, N. A. (2021). Beyond the individual: Governing AI's societal harm. *Internet Policy Review, 10*(3), 1–32.

Spruit, S. L., van den Poel, I., & Doorn, N. (2016). Informed consent in asymmetrical relationships: An investigation into relational factors that influence room for reflection. *NanoEthics, 10*, 123–138.

Stall, J. (2020). *Collectivize Facebook*. Retrieved August 18, 2022, from http://www.jonasstaal.nl/projects/collectivize-facebook/

Sunstein, S. (2003). *Why societies need dissent*. Harvard University Press.

Taylor, L., Floridi, L. & Van der Sloot, B. (2017). *Group privacy: New challenges of data technologies*. Springer.

Tombal, T. & Graef, I. (forthcoming 2023). The regulation of access to personal and non-personal data in the EU: From bits and pieces to a system? In B. Van der Sloot & S. van Schendel (Eds.), *The boundaries of data: technical, practical and regulatory perspectives*, Amsterdam University Press. Available as TILEC Discussion Paper No. 2022–019 at https://doi.org/10.2139/ssrn.4304148

Van Roermund, B. (2020). *Law in the first person plural. Roots, concepts, topics*. Edward Elgar Publishing.

Viljoen, S. (2021). A relational theory of data governance. *Yale Law Journal, 131*(2), 573–654.

Visagie, R., Beyers, S., & Wessels, J. (2019). Informed consent in Africa – Integrating individual and collective autonomy. In N. Nortje, R. Visagie, & J. Wessels (Eds.), *Social Science Research Ethics in Africa* (Vol. 7, pp. 165–179). Springer.

Wardrope, A. (2015). Relational autonomy and the ethics of health promotion. *Public Health Ethics, 8*(1), 50–62.

Westin, A. F. (1967). *Privacy and freedom*. Atheneum.

Wittrock, J. (2022). Liberalism, nationalism and religion: Multidimensional autonomy, trade-offs and analogies. Nations and Nationalism, 28(3), 1117-1130

Zimmerman, F. J. (2017). Public health autonomy: A critical reappraisal. *The Hastings Center Report, 47*(6), 38–45.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.