Information, Communication & Society

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/rics20

Regulating Big Tech expansionism? Sphere transgressions and the limits of Europe's digital regulatory strategy

Tamar Sharon & Raphaël Gellert

To cite this article: Tamar Sharon & Raphaël Gellert (2023): Regulating Big Tech expansionism? Sphere transgressions and the limits of Europe's digital regulatory strategy, Information, Communication & Society, DOI: 10.1080/1369118X.2023.2246526

To link to this article: https://doi.org/10.1080/1369118X.2023.2246526

Published online: 16 Aug 2023.

INFORMATION, COMMUNICATION & SOCIETY
https://doi.org/10.1080/1369118X.2023.2246526

Routledge
Taylor & Francis Group

Regulating Big Tech expansionism? Sphere transgressions and the limits of Europe's digital regulatory strategy

Tamar Sharon[a] and Raphaël Gellert[b]

[a]Department of Ethics and Political Philosophy and Interdisciplinary Hub for Digitalization and Society, Radboud University Nijmegen, Nijmegen, Netherlands; [b]Department of Private Law and Interdisciplinary Hub for Digitalization and Society, Radboud University Nijmegen, Nijmegen, Netherlands

ABSTRACT

The increasing power of Big Tech is a growing concern for regulators globally. The European Union has positioned itself as a leader in the stride to contain this expansionism; first with the GDPR and recently with a series of proposals including the DMA, the DSA, the AI Act, and others. In this paper we analyse if these instruments sufficiently address the risks raised by Big Tech expansionism. We argue that when this phenomenon is understood in terms of 'sphere transgressions' – i.e., conversions of advantages based on digital expertise into advantages in other spheres of society – Europe's digital regulatory strategy falls short. In particular, seen through the lens of sphere transgressions, Big Tech expansionism raises three risks in addition to well-known privacy and data protection risks, which this regulatory strategy does not properly address. These are: non-equitable returns to the public sector; the reshaping of sectors in line with the interests of technology firms; and new dependencies on technology firms for the provision of basic goods. Our analysis shows that this mismatch may be inherent to Europe's digital strategy, insofar as it focusses on data protection – while data is not always at stake in sphere transgressions; on political and civil rights – while socio-economic rights may be more at risk; and on fair markets – while the sectors being transgressed into by Big Tech, such as health and education, are not markets that require fairer competition, but societal spheres which need protection from market (and digital) logics.

ARTICLE HISTORY
Received 21 April 2023
Accepted 22 July 2023

KEYWORDS
Big Tech expansionism; sphere transgressions; EU digital regulatory strategy; technology regulation

1. Introduction

The increasing power of Big Tech is a growing source of concern for governments and regulators globally. In the past decade, large technology corporations including Apple, Alphabet, Meta, Amazon, Microsoft, Palantir and others, have not only consolidated their dominance in their original spheres of activity, but have begun to expand into new areas (Lopez et al., 2022; Sharon, 2016; van Dijck et al., 2019), including health

CONTACT Tamar Sharon tamar.sharon@ru.nl Department of Ethics and Political Philosophy and Interdisciplinary Hub for Digitalization and Society, Radboud University Nijmegen, Erasmusplein 1, 6525 HT Nijmegen, Netherlands
This article has been corrected with minor changes. These changes do not impact the academic content of the article.

and medicine, education, public administration, humanitarian aid and welfare, science, agriculture, banking, transportation, and even space exploration (for an overview see Stevens et al., 2022 and other articles in this special issue). During this time, the European Union (EU) has sought to position itself as a global leader in the stride to regulate digital innovation and its potential harms (European Commission, 2020, p. 6); beginning with the General Data Protection Regulation (GDPR) and most recently with a series of ambitious new legislative proposals, including the AI Act, the Digital Services Act (DSA), the Digital Markets Act (DMA), the Data Governance Act (DGA), the Data Act (DA), and the European Health Data Space (EHDS). In this paper we ask if this ambitious digital regulatory strategy sufficiently addresses the risks raised by Big Tech expansionism. We argue that when Big Tech expansionism is understood in terms of 'sphere trangressions' (Sharon, 2021a, 2021b; Walzer, 1983) – i.e., conversions of advantages based on digital expertise into advantages and dominance in other spheres of society – this digital strategy falls short.

The paper is structured as follows: In Section 2 we briefly describe the 'sphere transgressions' framework as a means of understanding Big Tech expansionism into new areas of society, before discussing the novel risks that this analytic lens makes visible. In addition to the privacy and data protection risks that are typically associated with the practices of tech corporations, we identify three additional risks. These include non-equitable returns (i.e., exploitation of public data without fair compensation); a gradual reshaping of critical sectors in line with the interests and practices of tech actors; and the creation of new dependencies on tech corporations for the provision of basic goods. Most of our examples come from the health and medical sector in light of the focus of a research project carried out by one of us on Big Tech expansionism into health (Sharon 2016, 2018). But we also draw on examples from other sectors, including education and agriculture. In Section 3 we first offer a brief description of the existing and proposed regulatory instruments that make up the EU's digital regulatory strategy before discussing how each of these instruments can or cannot address the identified risks of Big Tech expansionism as sphere transgressions.

Our analysis shows that while these legal instruments are helpful for addressing numerous risks ensuing from digital developments, none of them properly address the risks we identify in Section 2. We argue that this can be explained in terms of the two-pronged approach underlying Europe's digital regulatory strategy: on the one hand, a focus on fundamental rights and data protection as a means of protecting fundamental rights, and on the other, the development of fair (digital) markets. Concerning the first, data protection can only be a guarantor of fundamental rights when the collection and exchange of personal data is actually at stake. But, as we show, this is not necessarily the case in examples of sphere transgressions, which can be data-protection compliant and still raise other risks. Moreover, the catalogue of fundamental rights safeguarded through data protection (but to some extent also through the AI Act and the DSA) may be too narrow to encompass the broader socio-economic rights, such as health, education and welfare, which are at stake when tech corporations move into new sectors. Concerning the second focus, on fair markets, we argue that this promotes a view of sectors such as healthcare and education – which distribute basic social goods – as markets, the good governance of which requires no more than fair competition. We contend that this does little to protect the 'publicness' (Lopez et al., 2022) of public sectors susceptible

to Big Tech expansionism, and may actually increase opportunities for transgressions rather than thwart them.

In light of this, we suggest several new directions for regulation which may be required to address the risks of Big Tech expansionism. These include: increased regulation for socio-economic rights; a decoupling of digitalisation and marketisation, thereby ensuring that the transformation of traditional social goods into computational goods nonetheless precludes them from being reconfigured as market goods; and developing regulation that seeks not just to protect the fundamental rights of individual (data) subjects and fair markets, but that also seeks to protect societal spheres.

2. Sphere transgressions and their risks

We adopt the framework developed by Sharon and others (Sharon, 2021a, 2021b; Stevens et al., 2022; see also editorial of this special theme), which, drawing on Michael Walzer's (1983) theory of justice, understands Big Tech expansionism into new sectors as 'sphere transgressions'. From this perspective, advantages that tech companies have legitimately gained in what might be called the sphere of digital goods – namely digital know-how and expertise – are currently being translated into advantages in all spheres of society that undergo some form of digitalisation, from healthcare, to education, to agriculture. As Walzer warns, when advantages accrued in one sphere translate into advantages in another, there is a risk of domination of some members of society over others; for example, when wealth, an advantage accrued in the market sphere, is translated into advantages in other spheres, such as access to better healthcare or political power. Some things, in other words, are not – or should not be – for sale (Sandel, 2012). In the context of Big Tech expansionism from the sphere of digital goods into new ones, Sharon (2021a) argues that sphere transgressions based on such translations can raise the general spectre of domination and thus injustice. In particular, such translations are deemed illegitimate insofar as tech corporations do not have the domain expertise proportional to their new level of influence in these different societal spheres, and insofar as they are not accountable in the way that public sector actors are.

In the following sub-sections, we describe what we believe to be the main risks raised by Big Tech expansionism viewed through the lens of sphere transgressions. Our examples are drawn mostly from the health and medical sector, based on our previous research (Sharon 2016, 2018, 2021a). However, it is our contention that these risks are common to expansionism in all sectors in which tech companies are currently making inroads.

2.1. Privacy and data protection – the tip of the iceberg

First amongst these are privacy and data protection concerns. Many of the companies in question are notorious for their privacy policies and data sharing practices *within* their original sphere of activity. Such concerns may be even greater in the context of new spheres that these companies are getting involved in, where particularly sensitive personal data, such as medical data, or data collected on children in schools, are in question. This makes data subjects vulnerable to 'context transgressions' (Nissenbaum, 2010), whereby data collected in one context and under specific privacy norms, ends up in

another. In the health sphere, for example, we have already witnessed a few examples of how this can go wrong. In 2016, Google DeepMind became the centre of a data protection controversy when it was revealed that a data sharing partnership with three NHS hospitals allowed it to access identifiable health data on 1.6 million patients without their explicit consent (Powles & Hodson, 2017). An investigation conducted by the Information Commissioner's Office ruled that the data agreement violated data protection law (NHS, 2017). Similarly, in 2019, Google came under scrutiny when its partnership with Ascension, the second largest health system in the United States, granted the company access to over 50 million medical records (Copeland, 2019).

These examples notwithstanding, recent Big Tech expansionist initiatives into new spheres often *are* privacy and data protection friendly. A good example is the Apple/Google API for digital contact tracing.[1] At the outbreak of the COVID-19 pandemic, there was much discussion about the benefits of automating contact tracing using smartphones to help contain the pandemic. The risks of digital contact tracing were framed mostly in terms of privacy tied to the collection and storage of health and location data (Ienca & Vayena, 2020). In April 2020, in the midst of these discussions, Apple and Google jointly launched an API for contact tracing apps, which incorporated the stringent criteria defined by leading privacy experts for privacy friendly contact tracing, including the use of Bluetooth and decentralised storage. The initiative was applauded by privacy experts and data protection bodies alike (Whittaker, 2020) before being adopted by numerous countries around the world. Another example is the ResearchKit software, one of Apple's most ambitious health-related initiatives, which allows clinicians to carry out studies using the iPhone to collect health data. This software does not require collected data to flow to or through Apple. Instead, data is either kept on individual phones, or sent to data repositories where researchers can access it, pre-empting many data protection risks. Another example can be seen in a collaboration between Verily (an Alphabet subsidiary) and a university medical centre in the Netherlands for Parkinson's research, for which an infrastructure was built to ensure secure management of participants' data using novel data-protection-by-design techniques (Verheul & Jacobs, 2017).

One obvious reason for such privacy-friendly initiatives may be the already heightened focus on data protection in sectors such as health, into which Big Tech is expanding. But we suggest that this (also) has to do with evolving business models that are driving Big Tech expansionism. In many initiatives in new sectors, tech corporations are not collecting data in order to use it for targeted advertising – the business model we know well from ad tech and social media. The Apple ResearchKit, for example, will be a success when the software and the iPhone become widely used by clinicians for remote clinical trials – a form of research which is increasingly on the rise (see Stevens in this special issue). In other words, business models driving Big Tech expansionism may have more to do with monetising products, services and computational infrastructure (van Dijck et al., 2019) that will become valuable and possibly indispensable to the new spheres they are pushing into, rather than selling data. What's more, in such cases the focus on privacy and data protection can actually act as a smokescreen to other risks (Lopez et al., 2022; Sharon 2021a; Veale, 2020), and facilitate, rather than hinder, Big Tech expansionism. The lens of sphere transgressions is helpful here. Indeed, when

Big Tech expansionism is understood as illegitimate transgressions into new critical sectors, a number of risks beyond privacy and data protection become clear.

2.2. Non-equitable returns

The first of these is the risk that value generated by Big Tech's access to publicly funded datasets will not flow back to the public sector. While these companies may not necessarily be trading in data as a business model in their new spheres of activity, they are nonetheless using domain-specific data in many cases to develop products and services, such as diagnostic algorithms, which are proprietary, and which *can* be monetised. In the DeepMind–NHS collaboration mentioned above, DeepMind was using patient data from several hospitals to develop an app to help medical professionals identity patients at risk of acute kidney injury. The hospitals who were part of this agreement were able to use the app for free, but only for the duration of their initial contracts with DeepMind (five years) (Dickens, 2021). Other DeepMind AI research partnerships followed a similar pattern, by which hospitals had free access to resulting algorithmic technologies for the period of initial contracts, after which DeepMind would set a price for use and access. As Mustafa Suleyman, at the time head of AI at DeepMind, explained as early as 2016, 'right now it is about building the tools and systems that are useful and once users are engaged with them, we can figure out how to monetize them' (in Wakefield, 2016).

A similar business model motivated collaborations between the NHS and a number of tech firms during the COVID-19 pandemic, including Google, Amazon, Microsoft and Palantir. In exchange for some data analytics services, these companies could train their AI models on NHS data and were (originally) granted property rights (Fitzgerald & Crider, 2020). Such initiatives can be data protection compliant all the while raising the risk that the public sector ends up 'paying twice' (Mazzucato, 2018): once by funding the creation of datasets on which algorithms need to be trained, and once again when these algorithms are purchased or accessed for a fee. Much more needs to be done to ensure that monetary gains resulting from public-private partnerships are shared fairly, with equitable returns for taxpayers and patients (Bradley, 2022; Prainsack et al., 2022). This is not just the case for the healthcare sector, but for all sectors in which underfinanced public institutions are lured into partnerships with tech companies via incentives of seemingly no-strings-attached private investment.

2.3. Reshaping of critical sectors

A different type of risk that sphere transgressions raise pertains to the degree of influence that tech actors will have on a sphere; that is, the extent to which they may begin to reshape spheres in line with their own values and interests. Such an influence can be difficult to pinpoint and broad transformations to a sphere may happen in gradual, incremental steps. But it is not unreasonable to think that the more involved these actors become in critical sectors, and the more often they collaborate with traditional actors in critical sectors, the greater a role they will play in decisive processes, such as agenda setting. This may happen either when the personal interests of corporate leaders motivate involvement in a sphere or an area within a sphere, such as a specific disease, or when value-conflicts between tech and domain experts take place, and the former prevail.

2.3.1. Personal interests

An example of this, in the health and medical sphere again, is Alphabet's involvement in Parkinson's disease research, which spans a number of initiatives since 2010, including funding of research (Avey & Wokcicki, 2009), the development of smart products for Parkinson's patients, and the development of a wearable for Parkinson's research (Verily, 2017). Parkinson's is an incurable disease that afflicts millions worldwide, which certainly deserves the substantial attention it receives. However, Alphabet-related investments in Parkinson's can also be explained by Google co-founder Sergey Brin's personal interest in finding a cure to a disease he is at a heightened risk of developing himself, as a carrier of a gene which is linked to Parkinson's, something he has been open about (Brin, n.d.). Brin has channelled over $1.1 billion to fund Parkinson's research, mostly through his philanthropy 'Aligning Science Across Parkinson's'. Yet, as scholars of philanthropy (McGoey, 2015) point out, one of the problematic effects of philanthropy can be a distortion of the funding landscape, creating critical energy around one particular area and drawing away from others – for example, research into a rare genetic link. Moreover, while the burden of Parkinson's is such that Brin's philanthropy is of apparent value to global health, some tech billionaires are interested in advancing much more narrow research agendas. Top executives at Amazon, Palantir and Alphabet, for example, have been public about their interest in areas such as life extension and anti-ageing (Sample, 2022). The question here is not so much if this type of research may or may not be valuable. Rather, the question should be if, in a situation of constant resource scarcity for health and medical research, private actors should have an influence on research priorities, and which disease or disease sub-types become the focus of research.

2.3.2. Epistemic trespassing and technosolutionism

Spheres may also gradually be reshaped when clashes between tech actors and domain experts play out in favour of the interests of tech actors. With Google and Apple's development of the API for contact tracing for example, such a clash took place between the companies – who insisted on *decentralised* data storage – and some public health officials – who argued for *centralised* data storage. As mentioned, because decentralisation was equated with privacy-friendliness in the digital contact tracing debate, and because Google and Apple needed to demonstrate that their intervention would not be a threat to users' privacy, the duo was uncompromising about this point. A number of public health experts, however, argued at the time that there were good reasons for centralised data storage, such as overview of pandemic spread and cluster detection (Kelion, 2020). These voices were drowned out.

In this case, it is not so much the personal interests of tech executives which has an influence, but more about how the interests tech companies can have in imposing new – *digital* – practices, that are imported from outside and can affect the traditional concerns of a sphere, eventually also contribute to its reshaping. A good example of this can be taken from 'precision agriculture'. Precision agriculture is based on the results of self-learning algorithms which mine large volumes of data collected on farms and from the environment, usually by farm machinery equipped with sensors.[2] The datasets used here are not representative of all types of farming. Rather, they include data on a narrow selection of crops, namely those crops such as corn, canola and soy, which are grown on large farms which make use of heavy machinery and chemicals (Bronson,

2022). Left out of these datasets are crops grown by smaller peasant farms, which dominate globally and tend to be more biodiverse. As Bronson argues, in this way, precision agriculture creates a biased view of farming which is framed as commodity crop and capital-intensive. This reshapes the sphere, with important effects on our food system.

In this context, technosolutionism – the much-criticised logic by which tech enthusiasts go about redefining social phenomena as problems which technology can solve (Morozov, 2013) – can be understood as a form of 'epistemic trespassing' (Ballantyne, 2019) which can reshape a sphere. In the process, the original goods distributed within a specific sphere, be they healthcare, education, or food production, come to be redefined as problems that can be optimised computationally.

2.4. New dependencies

The final risk of Big Tech expansionism seen through the lens of sphere transgressions we point to is the emergence of new dependencies on tech firms for the provision of basic goods. An important avenue through which this can transpire is the expansion of tech firms' infrastructural power. Gürses and Dobbe (2020) distinguish between 'common infrastructure', traditional infrastructures such as water, sewage, and railway systems, and 'computational infrastructure', which they define as the global network of data centres, network infrastructure and mobile devices and platforms, which are becoming increasingly essential for the provision of digital services. Viewed from the infrastructural vantage point, it is misleading to see the products and services offered by these firms as standalones. They are, rather, elements of an ecosystem, which cannot be bought into without taking on the whole series of hardware, software, apps, cloud and operating system, which individual products (inter)operate with. As the ongoing digitalisation of societal sectors increasingly requires a computational infrastructure to run properly, this may lead to a deep dependence of public sectors on these firms for their main task, the provision of public services and goods. Yet, these actors are not held accountable to serving the public interest in the way that public actors are, nor are they upheld to public scrutiny in ways that enable redress (Taylor, 2021).

The digital contact tracing API that has already been referred to is a tell-tale example of just how dependent our daily lives have become on these computational infrastructures, and how this can affect a sector such as public health. Google and Apple's almost complete monopoly on smartphone operating systems meant that the very attempt to automate contact tracing with smartphone applications put public health authorities and governments at the mercy of Google and Apple's criteria (Veale, 2020). Another example is the extent to which both primary, secondary and higher education have become increasingly dependent on digital platforms and infrastructure, especially during the pandemic and its requirements of remote education (Fiebig et al., 2021; Kerssens & van Dijck, 2022). As these authors clearly indicate, one of the main issues at stake in primary and secondary school use of edtech and in the migration of universities to public clouds is autonomy and independence (not just data protection or privacy): be that in the form of the pedagogical autonomy of schools and teachers, or academic independence.

We now turn to the question if the regulatory instruments recently developed by the European Commission (EC) can properly address the risks of sphere transgressions we have identified in this section.

3. Sphere transgressions and the EU digital regulatory strategy

3.1. The EU's digital regulatory strategy: a short introduction

Since the late 2010s the EU has positioned itself as a global leader in the stride to regulate digital innovation and its potential harms. Various initiatives, beginning with the GDPR, followed by the AI Act, the DSA, the DMA, the DGA, the DA, and the EHDS, can be understood on the background of the EU's ambition to create a 'European digital leadership' (European Commission, 2020, p. 6).[3] In this regard, the EU's ambition is three-fold. It wants to promote innovation in digital technologies, while at the same time ensuring that such developments do not lead to – negative – market externalities (e.g., unfair or anti-competitive markets) and are also compatible with the EU's values and fundamental rights (European Commission, 2020, p. 1). In this sense, these new European initiatives can be understood as partaking of the EU's 'third way' concerning the development of digital technology, which differs from China's authoritarian and the US's business-oriented approaches (see European Commission, 2020, p. 2; JRC, 2018, pp. 12–13).

The *GDPR* (in force since 2018) aims at protecting the fundamental rights of individuals whose personal data are processed (GDPR, Article 1(1)(2)). It also aims at strengthening the EU's internal market (GDPR, Recital 2), which is seen as benefiting from digital technology (GDPR, Recital 7).

The *AI Act* (ongoing adoption process) aims at ensuring that AI systems that are placed on the EU internal market are considered safe, both from a physical and safety perspective as from a fundamental rights perspective (AI Act, Explanatory Memorandum, p. 3).

The *DSA* (adopted in 2022) aims at ensuring that hosting content providers and in particular online platforms do not infringe upon fundamental rights when delivering their services. It also aims to prevent dissemination of online illegal content (DSA, Recitals, 2, 3, 9).

The *DMA* (adopted in 2022) aims at ensuring that large online platforms, so-called 'gatekeepers' do not engage in new types of anticompetitive behaviours that are not always easily captured by traditional concepts of competition law (DMA, Explanatory Memorandum, p. 1, Recital 5).

The *DGA, DA* and *EHDS* can be grouped together, as their goal is to create a new EU internal market centred upon the exchange of data (EHDS, Explanatory Memorandum, p. 4). The main goal of the *DGA* (adopted in 2022) is to encourage the sharing of publicly (even subject to commercial or intellectual protection) and privately held data, against remuneration or for free under certain conditions ('data altruism') (DGA, Article 1, 2, 3). The *DA*'s (ongoing adoption process) overall goal is to maximise the use of and access to data with a specific focus upon the IoT context as far as access to data is concerned and cloud services as far as interoperability is concerned (Leistner & Antoine, 2022, p. 340), which is why its regulatory focus lies on regulating data portability, interoperability, access, and use (DA, Explanatory Memorandum, p. 1). Finally, the *EHDS* (ongoing adoption process) is to be seen as a more specific instrument focusing on the exchange of health data (EHDS, Explanatory Memorandum, p. 1), contrary to the DGA's and the DA's horizontal scope (EHDS, Explanatory Memorandum, p. 4).

The following sections discuss whether this EU digital regulatory strategy is able to adequately address each of the various risks raised by sphere transgressions.

3.2. The digital regulatory strategy vs. privacy and data protection risks

There are several ways in which the *GDPR* insufficiently addresses Big Tech expansionism's privacy and data protection risks (see, e.g., Gellert, 2021). One of these is 'creative compliance': a disconnect between compliance with rules on paper and the type of concrete protection that is achieved (McBarnet & Whelan, 1991). An example of 'creative compliance' enabling Big Tech expansionism is the Google DeepMind/NHS data sharing agreement mentioned earlier. Here, DeepMind and the Trust in question invoked 'direct care' (a principle which permits the use of patient data without explicit consent if those data are being used to treat the patient) in order to avoid gathering consent from the 1.6 million concerned patients. As Powles and Hodson argue (2017), the 'direct care' principle allowed DeepMind to legally bypass consent since it is unlikely that all those 1.6 million patients would ever actually be treated for acute kidney injury.

Another is how the GDPR's special rules on scientific research can offer a 'regulatory backdoor' to tech corporations interested in scientific research. As Marelli et al. (2021) have shown, these rules relax a number of key data protection principles such as those pertaining to data subject rights, limits on storage duration, and others. Moreover, the overly broad concept of scientific research enshrined in the GDPR might apply to (corporate) activities that would otherwise not fall under a more traditional understanding of scientific research (see Shabani & Yilmaz, 2022).

3.3. The digital regulatory strategy vs. non-equitable returns

Data protection's inability to address non-equitable returns is particularly displayed in the context of an important business model driving Big Tech expansionism into new sectors. Namely, the development of algorithms trained on domain-specific datasets, which are then turned into proprietary products (data analytics) that users must purchase. This is at play among others in the context of health data. As discussed, compliance with data protection need not stand in the way of the monetisation of the algorithms which are the result of that processing. A good example of this is the EHDS (Marelli et al. 2023). One of its ambitions is to facilitate the re-use of health data provided by European citizens and health providers for research and innovation (EHDS, Explanatory Memorandum, pp. 1–2). In this context, access to the EHDS by tech companies wanting to develop AI-based medical decision support tools is stated as one of the aims of the EHDS by the Commission itself.[4] In the face of these concerns the EHDS puts the emphasis on 'full compliance with the GDPR' (e.g., EHDS, Explanatory Memorandum, p. 3, Recital 3, Article 44). While this may effectively address risks associated with third party sharing of these data, it in no way addresses the risk of 'non-equitable returns', of companies accessing these data to create proprietary algorithms. On the contrary, the Proposal encourages the use of these data for innovation by industry actors. Yet, the question of how any profits, services or intellectual property generated by industry will flow back to EU citizens and health providers whose data are being accessed is left unanswered.[5]

Neither do the other instruments properly address this risk. The *AI Act*'s goal to ensure that algorithms and AI systems being sold and used are reasonably free from risks in terms of data protection, discrimination, etc. (AI Act, Recital 15) would do

very little to address issues concerning the transformation of algorithms trained on freely made available data into proprietary goods.

The *DSA* is also silent concerning the manner in which online platforms train their algorithms on their users' data, which in turn they use for monetisation and profitmaking purposes through user engagement (see, e.g., Beauvisage & Mellet, 2020). Rather, it limits itself to for instance rules pertaining to the transparency of algorithmically produced search results (DSA, Article 27), or the societal risks created by the personalisation of online content (see, e.g., DSA, Articles 34–35).

Nor is the *DMA* concerned with the way in which businesses develop their algorithms or software. The concept of fair market conditions on which it relies (see, Petit, 2021, pp. 535–537) assumes that charging for digital services is a fair market practice, and what matters most is ensuring a fair level-playing field between various businesses who have asymmetrical market power (see DMA, Explanatory Memorandum, pp. 1–3).

The *DGA* is probably the most relevant instrument here, especially considering its provisions on 'data altruism', which allow for the free sharing of data provided the goal pursued by the processing entity is one of general interest (e.g., healthcare, combating climate change, improving mobility and the provision of public services, or scientific research more broadly) (DGA, Article 2(16), 16) (Ruohonen & Mickelsson, 2021, p. 3). However, it remains silent with regard to the products that will be developed on the basis of this data and the condition of access thereto. It may thus aggravate the problem of non-equitable returns.

In light of the *DA*'s overall goal of promoting data sharing (DA, Explanatory Memorandum, p. 1), and therefore creating new data markets (Leistner & Antoine, 2022, p. 344), it does not directly address the issue either.

3.4. The digital regulatory strategy vs. reshaping of critical sectors

As mentioned in Section 3.1, one of the main goals of the EU digital regulatory strategy is to prevent anti-competitive digital markets. In this sense, it aims (at least theoretically) to avoid the type of dominance based on personal interests discussed in Section 2.3.1. That being said, it will not be helpful to counter the epistemic trespassing that accompany sphere transgressions, and which can contribute to a profound reshaping of sectors. Indeed, ensuring that personal data are processed fairly (*GDPR*), that only safe AI systems are placed on the market (*AI Act*), or that illegal content is not shared online (*DSA*), will not address the reshaping of traditional goods as computationally optimisable problems. After all, the GDPR, the AI Act and the DSA never dispute the imperative of nurturing the internal market on the basis of digital technology. On the contrary, they all embrace it, provided some fundamental rights safeguards are complied with.

The most relevant instrument in this regard is the *DMA*, given its goal to ensure a fair and competitive market and thus to avoid dominant market positions and 'higher prices, lower quality, as well as less choice and innovation to the detriment of European consumers' (DMA, Explanatory Memorandum, p. 1, Recitals 2, 4, 5). Yet, avoiding situations of market dominance does not change the fact that the point is for consumers to 'reap the full benefits of the (…) digital economy' (DMA, Explanatory Memorandum, pp. 2–3). If the digital economy is about the increasing transformation of public goods into computational goods, then here too the problem is aggravated rather than addressed. The fact

that computational goods are provided by a myriad of competitive tech companies rather than by one – or a few – dominant ones changes nothing.

The *DA* also strives for fairer markets with no entry barriers by ensuring that users would be able to port their data more easily from one cloud service to another (Leistner & Antoine, 2022, p. 340). It is thus vulnerable to the same critique. Further, its explicit ambition to create new markets on the basis of accessed data (Data Act, Explanatory Memorandum, p. 3) can be seen as also reinforcing the problem since it would lead to the transformation of additional goods into computational goods.

The *DGA* suffers from the same flaws, insofar as it encourages the sharing of data. Of particular relevance are the provisions on data altruism, which could lead to more epistemic trespassing under the guise of progress and innovation in the general interest. This can be clearly unearthed via the provisions concerning the so-called 'European Data Innovation Board'. Its task among others is to 'propose guidelines for common European data spaces', the goal of which is to share data for purposes of the development of new products or scientific research (DGA, Article 30(h)).

3.5. The digital regulatory strategy vs. new dependencies

Ensuring that personal data are processed fairly will not address the path-dependencies stemming from the growth of computational infrastructure since the business model is less about monetising data than developing computational infrastructure on which certain sectors and sub-sectors will run (Section 2.4). Similar considerations apply to the *AI Act*, and its focus on the placing of safe AI systems on the market.

The *DSA* and the *DMA* are probably the most relevant instruments here, given that they are the ones regulating online platforms, which have been equated with computational infrastructure (Cohen, 2019) – either in their capacity as information society services allowing for the transmission of information (DSA), or in their capacity as gatekeeper in the context of the provision of the core platform services (DMA) (see Sabeel Rahman, 2018, p. 242). However, here too these initiatives fall short. The DSA provides for more accountability and responsibilisation of online platforms through for instance novel provisions on content moderation or content curation (DSA, Articles 16, 25–27). Regardless of their purported efficiency, the point is they do nothing to address the way in which information is shared online from an infrastructural viewpoint. On the contrary, this phenomenon is encouraged provided the DSA provisions are complied with (DSA, Explanatory Memorandum, pp. 2–3). The DMA, on the other hand, addresses gatekeeping issues, a proxy pointing to watered-down monopolistic types of situations in digital markets (Petit, 2021, p. 532). Monopolistic situations have historically had a lot to do with issues of infrastructural dependency especially in the context of public utilities (see, Sabeel Rahman, 2018, p. 238). However, instead of focusing on the (public) utility nature of online platforms, which could lead to further-reaching (public-law inspired) regulatory measures, such as preventing online platforms to access certain markets or to force them to get rid of certain assets, it adopts a competition law approach and its vaguer and less far-reaching goal of 'fair and contestable' markets (Petit, 2021, p. 531).[6]

The fact that one of the *DA*'s aims is to improve interoperability for cloud services (see, Leistner & Antoine, 2022, p. 341) is telling, since cloud is a key computational

infrastructure, where the risk of loss of control of public authorities has already been evidenced (see, Privacy Company, 2019). As discussed, in the context of education, the use of cloud services is an issue of (educational) autonomy. Making cloud services more interoperable will not address this.

The *DGA* is likely to promote more dependencies on tech corporations as well. On the one hand, tech corporations will have a competitive advantage when it comes to acquiring public sector data against compensation (more financial resources). On the other hand, granting them the data for free in the context of data altruism can be seen as an encouragement to enable them to transform more infrastructure into a computable one.

4. Conclusion

To conclude this contribution, we would like to sketch a few insights from the observed shortcomings of the upcoming EU digital legal framework for regulating the risks raised by Big Tech expansionism understood as sphere transgressions. A starting point concerns the EU's general regulatory approach, which can be traced back to its goal of realising a 'European digital leadership' (EC, 2020, p. 6). The EU clearly sees digitalisation as an opportunity to be seized, which can lead to citizen well-being, help address various societal challenges, such as climate change, or create value, provided this is done in a responsible way. That is, as long as digital technologies are used in societally beneficial ways, do not lead to market externalities (e.g., unfair or anti-competitive markets), and are compatible with EU values and fundamental rights (EC, 2020). Digitalisation is upheld here as a solution to a number of societal problems, which can simultaneously generate economic growth and value. The challenge then resides in supporting digitalisation which is in line with EU values and fundamental rights.

The linear vision implied in this approach, of science and innovation solving societal problems and leading to societal progress, has long been criticised for being overly simplistic in terms of its promises (i.e., innovation journeys are never linear), but also in terms of the societal configurations it assumes and contributes to (i.e., focus upon competitiveness and economic impact, which in turn empowers certain entrenched and already powerful actors) (Felt et al., 2007, p. 22). This paper contributes to this critique, by showing the inability of the EU's recent digital regulatory strategy to adequately take into account known and novel risks raised by Big Tech expansionism understood in terms of sphere transgressions.

Our analysis shows that the EU's digital regulatory strategy does not do enough to address these risks, and in many cases may further exacerbate them. We believe this can be explained in terms of the two main orientations that this strategy undertakes – on the one hand, a focus on fundamental rights (and in particular data protection as a means of protecting fundamental rights), and on the other developing fair (digital) markets – each of which presents important shortcomings in relation to sphere transgressions.

Concerning the first, data protection rules can only guarantee fundamental rights when the collection and exchange of personal data is actually at stake. But, as we show, this is not necessarily the case in examples of sphere transgressions, which can be data-protection compliant all the while raising risks of non-equitable returns, reshaping of sectors and new dependencies (similar considerations apply to the DSA and AI

Act). Moreover, the fundamental rights that the proposed legal instruments seek to protect are all predominantly civil and political freedoms – anti-discrimination, freedom of speech and information, privacy, etc.[7] – while it is questionable whether these rights can address some of the implicit societal configurations that underpin the linear model of innovation which enables sphere transgressions. This begs the question as to whether fundamental rights can really achieve the ideals (i.e., justice, etc.) they promote or whether they are a mere '250-year-old perpetual utopia' (Gutwirth & De Hert, 2021).

Second, if the focus on (first generation) fundamental rights is problematic, so is the second orientation of the EU digital strategy: the focus on fair and competitive markets. This focus allegedly stems from the EU's vision of technological innovation, but also from its limited competence to regulate (i.e., the EU's competences remain predominantly about the internal market even though its fundamental rights competences have expanded since the Lisbon Treaty (see, e.g., Muir, 2014)). Nonetheless, the emphasis on (fair) markets is not only unable to adequately address the risks of Big Tech expansionism into new sectors in terms of non-equitable returns, a reshaping of sectors and new dependencies. It may also create *new* risks. Indeed, the regulatory anchoring in the internal market rationale entails that digitalisation be viewed, to some extent, as a market issue – be it a product in the case of the AI Act, a service in the case of the DSA and DMA, or the source of value creation in the case of the GDPR, DGA, Data Act, and EHDS. Doing so simultaneously generates a novel risk. Namely of reconfiguring (and regulating) digitalisation-related issues solely as market issues. This is problematic since digitalisation, as a transversal technology, applies to many sectors that are not – and in our opinion *should* not – be treated as markets, insofar as they provide access to basic social goods (e.g., healthcare, education, public administration, etc.). This raises the spectrum of a double transgression, from the sphere of digital goods *and* from the sphere of the market.

Finally, we would like to emphasise that our aim is not to construct a facile critique of the EU's digital regulatory strategy. We acknowledge that these instruments address many relevant issues and achieve many positive things. Similarly, we understand that the EU's competences are constrained by the Treaty on the Functioning of the EU, and that within this ambit, it produces a commendable effort to address some of the major digitalisation-related risks our societies face. Our point, rather, is that what is left unaddressed, '*hors champ*', by this regulatory strategy requires attention.[8] By leaving unquestioned a number of assumptions on the role and place that digital technology has in European society, the EU runs the risk of aggravating the dangers associated with sphere transgressions. In this regard, one may wonder whether the EU is the best institutional framework to regulate these technologies if all it can do is improve the way in which such technology is developed, rather than being able to decide whether digital technology is the best way forward in all situations.

This raises the question as to what other regulatory alternatives are available. We believe our analysis points to several new directions which would be required to better address sphere transgressions and possibly digitalisation in general. First, an awareness that, when it comes to digital harms, privacy and data protection are just the tip of the iceberg, and that we should be wary of how this focus diverts attention from broader societal transformations which take place gradually and incrementally. Second, the focus on first generation fundamental rights might need to make way to so-called

second-generation fundamental rights (also referred to as socio-economic rights), such as the right to health, housing, education, employment, etc. (Dickens, 2021; Niklas, 2022). Despite their less established legal existence, these rights may be more attuned to – and better able to address – the societal configurations within which the current models of digital innovation are embedded, and in doing so better address the risks created by sphere transgressions. Third, an understanding that when fairness – and its counterpart, domination – are understood predominantly as market fairness and market domination, basic social goods risk being redefined as market goods. Fourth, while digitalisation and marketisation currently tend to go hand in hand, this alliance is not inevitable, and we should do good to decouple them. Finally, as increasing sectors of society become digitised, and as the digital services and expertise of tech actors become increasingly valuable and coveted, we may need to think of how regulation can protect not just the fundamental rights of individual (data) subjects and fair markets, but how to protect spheres.

Notes

1. https://covid19.apple.com/contacttracing.
2. Currently the largest actors involved in precision agriculture are traditional agricultural firms, but Palantir, Google, Microsoft, the Gates Foundation, Huawei, IBM have all begun moving into this sector (see https://www.sphere-transgression-watch.org).
3. This is of course reminiscent of Bradford's work on the so-called 'Brussels effect' (Bradford, 2021).
4. See, e.g., question no. 7, example 2 on the 'Questions and answers' page, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_22_2712.
5. Bietti (2020) has voiced similar concerns surrounding the regulation of platforms through the regulation of data processing.
6. On the interface between public utilities regulation and competition law in the EU, see for instance Monti (2008); in the US (where the term antitrust is used instead of competition), see for instance Sabeel Rahman (2018, p. 236).
7. On the concept of human rights generally, among an overwhelming literature, see for instance Sudre (2016).
8. Not to mention that there are of course other angles of critique of this regulatory strategy, see for instance Streinz (2021).

Disclosure statement

No potential conflict of interest was reported by the author(s).

Funding

This work was supported in part by the European Research Council under Grant number 804985.

Notes on contributors

Tamar Sharon is Professor of Philosophy, Digitalization and Society, Chair of the Department of Ethics and Political Philosophy and Co-Director of the Interdisciplinary Hub for Digitalization and Society (iHub) at Radboud University, Nijmegen. Her research explores how the increasing digitalisation of society destabilises public values and norms, and how best to protect them. She

is a member of the European Commission's European Group on Ethics in Science and New Technologies. [email: tamar.sharon@ru.nl]

Raphaël Gellert is an assistant professor in ICT and private law at Radboud University, where he is a member of the Radboud Business Law Institute, and of the Interdisciplinary Hub for Digitalization and Society (iHub). The core of his research revolves around the regulation of technologies, and in particular digital technologies, which he conducts in an interdisciplinary fashion. He is the author of *The Risk-Based Approach to Data Protection*, published in 2020 by Oxford University Press. [email: raphael.gellert@ru.nl]

References

Legislation

Proposal of the European Commission for a Regulation of the European Parliament and of the Council on harmonized rules on fair access to and use of data (2022) (Data Act).

Proposal of the European Commission for a Regulation of the European Parliament and of the Council on the European Health Data Space (2022) (EHDS).

Proposal of the European Commission for a Regulation of the European Parliament and of the Council Laying down Harmonised Rules on Artificial Intelligence (2021) (AI Act).

Regulation (EU) 2016/679 of 27 April 2016 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 (GDPR) [2016] OJ L 119/1.

Regulation (EU) 2022/2065 of 19 October 2022 of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) [2022] OJ L 277/1.

Regulation (EU) 2022/1925 of 14 September 2022 of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) [2022] OJ L 265/1.

Regulation (EU) 2022/868 of 30 May 2022 of the European Parliament and of the Council on European data governance (Data Governance Act) [2022] OJ L 152/1.

Literature and other sources

Avey, L., & Wokcicki, A. (2009, March 11). *A new approach to research: The 23andMe Parkinson's Disease Initiative*. https://blog.23andme.com/articles/a-new-approach-to-research-the-23andme-parkinsons-disease-initiative

Ballantyne, N. (2019). Epistemic trespassing. *Mind; A Quarterly Review of Psychology and Philosophy*, *128*(510), 367–395. https://doi.org/10.1093/mind/fzx042

Beauvisage, T., & Mellet, K. (2020). Datassets: Assetizing and marketizing personal data. In *Assetization turning things into assets in technoscientific capitalism*. https://doi.org/10.7551/mitpress/12075.001.0001

Bietti, E. (2020). Platform power and the limits of the informational turn. *Pace Law Review*, *40*(1), 310. https://doi.org/10.58948/2331-3528.2013

Brin, S. (2008, September 18). LRRK2. *Too*. http://too.blogspot.com

Bradford, A. (2021). *The Brussels effect: How the European union rules the world*. Oxford University Press.

Bradley, S. H., Hemphill, S., Markham, S., & Sivakumar, S. (2022). Healthcare systems must get fair value for their data. *BMJ*, 377, e070876.

Bronson, K. (2022). *The immaculate conception of data: Agribusiness, activists and their shared politics of the future*. McGill-Queen's University Press.

Cohen, J. E. (2019). *Between truth and power: The legal construction of information capitalism*. Oxford University Press.

Copeland, R. (2019, November 11). Google's 'Project Nightingale' gathers personal health data on millions of Americans. *WSJ*. https://www.wsj.com/articles/google-s-secret-project-nightingale-gathers-personal-health-data-on-millions-of-americans-11573496790

Dickens, A. (2021). *The right to health implications of data-driven health research partnerships* [Unpublished doctoral dissertation]. University of Essex.
European Commission. (2020). Shaping Europe's digital future. https://doi.org/10.2759/48191
Felt, U., Wynne, B., Callon, M., Gonçalves, M. E., Jasanoff, S., Jepsen, M., Joly, P., Konopasek, Z., May, S., Neubauer, C., Rip, A., Siune, K., Stirling, A., & Tallachini, M. (2007). Taking European Knowledge Society Seriously: Report of the Expert Group on Science and Governance to the Science, Economy and Society Directorate, Directorate-General for Research, European Commission.
Fiebig, T., Gürses, S., Gañán, C., Kotkamp, E., Kuipers, F., Lindorfer, M., Prisse, M., & Sariet, T. (2021, April 19). *Heads in the clouds: Measuring the implications of universities migrating to public clouds*. https://arxiv.org/abs/2104.09462
Fitzgerald, M., & Crider, C. (2020, May 7). We need urgent answers about the massive NHS COVID data deal. *Open Democracy*. https://www.opendemocracy.net/en/ournhs/we-need-urgent-answers-about-massive-nhs-covid-data-deal/
Gellert, R. (2021). Personal data's ever-expanding scope in smart environments and possible path(s) for regulating emerging digital technologies. *International Data Privacy Law*, *11*(2), 196–208. https://doi.org/10.1093/idpl/ipaa023
Gürses, S., & Dobbe, R. (2020, February 18). *Programmable infrastructures*. TUDelft. https://www.tudelft.nl/tbm/programmable-infrastructures
Gutwirth, S., & De Hert, P. (2021). Human rights: A secular religion with legal crowbars. From Europe with hesitations. *National Law School of India Review*, *33*(2), 420–462.
Ienca, M., & Vayena, E. (2020). On the responsible use of digital data to tackle the COVID-19 pandemic. *Nature Medicine*, *26*(4), 463–464. https://doi.org/10.1038/s41591-020-0832-5
JRC. (2018). *Artificial intelligence: A European perspective*.
Kelion, L. (2020, April 27). NHS rejects Apple-Google coronavirus app plan. *BBC*. https://www.bbc.com/news/technology-52441428
Kerssens, N., & van Dijck, J. (2022). Governed by edtech? Valuing pedagogical autonomy in a platform society. *Harvard Educational Review*, *92*(2), 284–303. https://doi.org/10.17763/1943-5045-92.2.284
Leistner, M., & Antoine, L. (2022). Attention, here comes the EU data Act! A critical in-depth analysis of the commission's 2022 proposal. *Jipitec*, *13*(3), 339–349.
Lopez, J., Martin, A., Ohai, F., de Souza, S., & Taylor, L. (2022). Digital disruption or crisis capitalism? Technology, power and the pandemic. https://doi.org/10.26116/gdj-euaifund
Marelli, L., Testa, G., & van Hoyweghen, I. (2021). Big Tech platforms in health research: Re-purposing big data governance in light of the General Data Protection Regulation's research exemption. *Big Data & Society*. https://doi.org/10.1177/20539517211018783
Marelli, L., Stevens, M., Sharon, T., Hoyweghen, I. V., Boeckhout, M., Colussi, I., Degelsegger-Márquez, A., El-Sayed, S., Hoeyer, K., van Kessel, R., Zając, D. K., Matei, M., Roda, S., Prainsack, B., Schlünder, I., Shabani, M., & Southerington, T. (2023). The European health data space: Too big to succeed? *Health Policy*. https://doi.org/10.1016/j.healthpol.2023.104861
Mazzucato, M. (2018). *The value of everything*. Penguin Books.
McBarnet, D., & Whelan, C. (1991). The elusive spirit of the law: Formalism and the struggle for legal control. *The Modern Law Review*, *54*(6), 848–873. https://doi.org/10.1111/j.1468-2230.1991.tb01854.x
McGoey, L. (2015). *No such thing as a free gift: The gates foundation and the price of philanthropy*. Verso.
Monti, G. (2008). Managing the intersection of utilities regulation and EC Competition Law. In *LSE Working Papers* (8/2008; LSE Law, Society and Economy Working Papers). https://doi.org/10.2139/ssrn.1111969
Morozov, E. (2013). *To save everything click here.* Public Affairs.
Muir, E. (2014). Fundamental rights: An unsettling EU competence. *Human Rights Review*, *15*(1), 25–37. https://doi.org/10.1007/s12142-013-0295-x
NHS. (2017). Information Commissioner's Office (ICO) investigation. https://www.royalfree.nhs.uk/patients-visitors/how-we-use-patient-information/information-commissioners-office-ico-investigation-into-our-work-with-deepmind/

Niklas, J. (2022). *Social rights and data technologies*. Data Justice Lab, Cardiff University.
Nissenbaum, H. (2010). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.
Petit, N. (2021). The proposed digital markets act (DMA): A legal and policy review. *Journal of European Competition Law and Practice*, *12*(7), 529–541. https://doi.org/10.1093/jeclap/lpab062
Powles, J., & Hodson, H. (2017). Google DeepMind and healthcare in an age of algorithms. *Health and Technology*, *7*(4), 351–367. https://doi.org/10.1007/s12553-017-0179-1
Prainsack, B., El-Sayed, S., Forgó, N., Szoszkiewicz, L., & Baumer, P. (2022). *Data solidarity*. The Lancet and Financial Times Commission. https://www.governinghealthfutures2030.org/wp-content/uploads/2022/12/DataSolidarity.pdf
Privacy Company. (2019). *New DPIA on Microsoft Office and Windows software: still privacy risks remaining (long blog)*. https://www.privacycompany.eu/blogpost-en/new-dpia-on-microsoft-office-and-windows-software-still-privacy-risks-remaining-long-blog
Ruohonen, J., & Mickelsson, S. (2021). *Reflections on the Data Governance Act. 2022*, 1–10. https://doi.org/10.48550/arXiv.2302.09944
Sabeel Rahman, K. (2018). Regulating informational infrastructure: Internet platforms as the new public utilities. *Georgetown Law Technology Review*, *2*(2), 234–251.
Sample, I. (2022, February 17). If they could turn back time: How tech billionaires are trying to reverse the ageing process. *The Guardian*. https://www.theguardian.com/science/2022/feb/17/if-they-could-turn-back-time-how-tech-billionaires-are-trying-to-reverse-the-ageing-process
Sandel, M. (2012). *What money can't buy: The moral limits of markets*. Farrar, Straus and Giroux.
Shabani, M., & Yilmaz, S. (2022). Lawfulness in secondary use of health data. *Technology and Regulation*, 2022, 128–134. https://doi.org/10.26116/techreg.2022.013
Sharon, T. (2016). The Googlization of health research: From disruptive innovation to disruptive ethics. *Personalized Medicine*, *13*(6), 563–574.
Sharon, T. (2018). When digital health meets digital capitalism, how many common goods are at stake? *Big Data & Society*. https://doi.org/10.1177/2053951718819032
Sharon, T. (2021a). Blind-sided by privacy? Digital contact tracing, the Apple/Google API and big tech's newfound role as global health policy makers. *Ethics and Information Technology*. https://doi.org/10.1007/s10676-020-09547-x
Sharon, T. (2021b). From Hostile Worlds to multiple spheres: Towards a normative pragmatics of justice for the Googlization of health. *Medicine, Health Care & Philosophy*. https://doi.org/10.1007/s11019-021-10006-7
Stevens, M., Sharon, T., van Gastel, B., Hoffman, A., Kraaijeveld, S., & Siffels, L. (2022). *Sphere transgression watch*. Distributed by iHub, http://www.sphere-transgression-watch.org
Streinz, T. (2021). The evolution of European data Law. In Paul Craig & Gráinne de Búrca (Eds.), *The evolution of EU Law* (pp. 902–936). Oxford University Press.
Sudre, F. (2016). *Droit européen et international des droits de l'homme* (13ème édit). Presses Universitaires de France - puf.
Taylor, L. (2021). Public actors without public values. *Philosophy and Technology*, *34*(4), 897–922. https://doi.org/10.1007/s13347-020-00441-4
van Dijck, J., Poell, T., & de Waal, M. (2019). *The platform society: Public values in a connective world*. Oxford University Press.
Veale, M. (2020, July 1). Privacy is not the problem with the Apple-Google contact-tracing toolkit. *The Guardian*. https://www.theguardian.com/commentisfree/2020/jul/01/apple-google-contact-tracing-app-tech-giant-digital-rights
Verheul, E., & Jacobs, B. (2017). Polymorphic encryption and pseudonymisation in identity management and medical research. *NAW*, *5*(18), 168–172.
Verily. (2017, April 14). *Introducing Verily Study Watch*. https://verily.com/blog/introducing-verily-study-watch/
Wakefield, J. (2016, September 23). Google DeepMind: Should patients trust the company with their data? *BBC News*. http://www.bbc.com/news/technology-37439221?post_id¼1038675936156065_1277197572303899#_¼_
Walzer, M. (1983). *Spheres of justice: A defense of pluralism and equality*. Basic Books.

Whittaker, Z. (2020, April 20). Hundreds of academics back privacy-friendly coronavirus contact tracing apps. *TechCrunch*. https://techcrunch.com/2020/04/20/academics-contact-tracing/?guce_referrer = aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig = AQAAABPb8I0cVVxM60JP5vVeAotDhzAmaXozNJ3KnXwcF5KKD_HdKhr-Gz-PEZC2uVI8PgY4WzZ5WtKWLVow6_e1ZjgISqz0vlPMoTW78WPvjmupok0b4k8cHS_Yudk5rtbIyi9OwNdwubEShXFY7P9iDhnFUeOBemSSl2AWpIWQ3Yem&guccounter = 2