The ‘Datasphere’, Data Flows beyond Control, and the Challenges for Law and Governance

Jean-Sylvestre Bergé
Professor of Law, University of Lyon, Institut universitaire de France
jsberge@gmail.com

Stéphane Grumbach
Senior Scientist at Inria; Director of IXXI, the Complex Systems Institute, ENS Lyon
stephane.grumbach@inria.fr

Vincenzo Zeno-Zencovich
Professor of Comparative Law, Roma Tre University
zencovic@uniroma3.it

Abstract

The flows of people, goods and capital, which have considerably increased in recent history, are leading to crises (e.g., migrants, tax evasion, food safety) which reveal the failure to control them. Much less visible, and not yet included in economic measurements, data flows have increased exponentially in the last two decades, with the digitisation of social and economic activities. A new space – Datasphere – is emerging, mostly supported by digital platforms which provide essential services reaching half of the world’s population directly. Their control over data flows raises new challenges to governance, and increasingly conflicts with public administration.

In this paper, we consider the need and the difficulty of regulating this emerging space and the different approaches followed on both sides of the Atlantic. We distinguish between three situations. We first consider data at rest, which is from the point of view of the location where data are physically stored. We then consider data in motion, and the issues related to their combination. Finally, we investigate data in action, that is data as vectors of command of legal or illegal activities over territories, with impacts on economy and society as well as security, and raise governance challenges.

The notion of ‘Datasphere’ proposes a holistic comprehension of all the ‘information’ existing on earth, originating both in natural and socio-economic systems, which
can be captured in digital form, flows through networks, and is stored, processed and transformed by machines. It differs from the 'Cyberspace', which is mostly concerned with the networks, the technical instruments (from software and protocols to cables and data centers) together with the social activities it allows, and to what extent they could/should be allowed.

The paper suggests one – out of the many possible – approach to this new world. Clearly it would be impossible to delve in depth into all its facets, which are as many as those of the physical world. Rather, it attempts to present how traditional legal notions could be usefully managed to put order in a highly complex environment, avoiding a piecemeal approach that looks only at details.

Keywords


1 Introduction

The development of information and communication technologies, such as smartphones and the numerous sensors spread across the public and private space, has promoted the digitalisation of a considerable quantity of data\(^1\) on human activity and on the world around us in general. Units of measurement such as zetta, denoting thousands of billions of billions,\(^2\) have been introduced to designate these orders of magnitude, known in the realm of natural sciences, but until recently absent from the realm of human activity. The quantity of data has increased exponentially in accordance with a law similar to Moore's law, which in 1965 predicted that computers' capacity would double every 18 months.

The data, closely linked to the algorithms supporting them, make up a new space – a digital sphere – which constitutes a reflection of the physical world, containing both the objects we find in it (buildings, roads, plants, animals and landscapes) and the traces of the activity occurring in the physical world, such as our position at any given moment, our exchanges, the temperature of our homes, financial movements and movements of goods or road traffic.

---

\(^1\) We shall use the term 'data' in the sense of any information in digital form that can be transmitted or processed.
This digital sphere allows activities that did not previously exist to be created, such as search engines for accessing knowledge. However, it also enables activities that have always been assumed by players in the physical world to be transferred into the digital sphere, such as mediation in the transport business. It is mostly supported by digital platforms, which provide essential services reaching now half of the world’s population directly.

The control over data flows of the main actors of the digital sphere raises new challenges to governance, and increasingly conflicts with public administration. Controlling flows is by no means a new issue, though. The flows of people, goods and capital, which have considerably increased in recent history, are leading to crises (e.g., migrants, tax evasion, food safety) which reveal the failure to fully control them. But the flow of data, which is consubstantial with the digital sphere, is much less visible; it is not yet included in economic metrics of international organisations, for instance.

These flows have to be considered with scrutiny, under the assumption of total flow without control. People (physical or moral), goods (tangible or intangible), including in extensive forms, services and capital circulate within and between territories. This circulation, consubstantial with the ordering of the world, has acquired new dimensions: speed, diversity and volume, which reached levels hitherto unparalleled. We can reasonably think that the phenomenon can only be amplified.

The movement of people and goods is total in that it mobilises the attention and behaviour of all public and private actors in defined local, national or international contexts (States, companies, citizens) which contribute, voluntarily or involuntarily, to the phenomenon.

Flows have a dimension beyond control in the sense that in specific or temporary situations they escape all or part of the control of the actors, including those who lead them. This circulation beyond control is generated within its own sphere, its positive and negative circuits, legal and illegal.

It has been shown\(^2\) that the digital sphere, considered as a new space, questions the law on the way in which it comprehends spaces in the widest sense of the term. The solution can be sought in the constructions of public international law. There exists an international regime of spaces where international law adopts an overall approach to land space, the sea, international channels, rivers and lakes, the skies, or outer space.

The question is whether the digital sphere requires the same ‘need of law’,3 justifying an overall approach in terms of ‘space’. Answers have been given in the specific context of the Internet, for example. The image of ‘cyberspace’, its ambitions for independence,4 its own regulatory regimes and the types of players involved undoubtedly feed a wide-ranging debate on the subject.5

However, what about the digital sphere, with a larger extension potentially covering the whole of human activity on the planet? Has there been a proposal for a global study to identify that sphere as a space, potentially subject to one or more legal regimes? It seems that the answer has to be negative.

Legal constructions do not yet recognise the digital sphere as a new space. Unlike the other natural spheres of earth (such as the lithosphere, the hydrosphere, the atmosphere), the digital sphere, or to be more precise, the datasphere (henceforth, ds), is not yet considered to create a specific field of human activity into which the law could intervene and organise.6

Two new types of relationship would basically be formed from the emergence of a new space. First, the ds triggers the creation of new relationships

---


5 In 2006 the UN established an Internet Governance Forum (IGF) with the aim of facilitating inclusive, productive discussions on Internet-related public policy issues from a general perspective. Among the topics it has examined are those of Big Data and the protection of personal data.

6 The well-known notion of cyberspace is focused mainly on what might be called the engineering elements of this new ‘space’: networks, whether physical or wireless, protocols (e.g. the TCP/IP protocol used in the Internet), identification rules (domain names, URLs) where a significant role is played by the Internet Corporation for Assigned Names and Numbers (ICANN) and the rights and duties of public and private entities and of individuals. The cyberspace also includes the social interactions allowed by the infrastructures. In this paper, the focus is on data as the digital expression of practically any existing element of the physical world and of any activity (human, animal, natural, automated) that happens within it. This data is mostly collected through devices which allow the data to flow to the networks, but there are many other modes and ‘places’, such as closed networks (i.e. those of payment systems), or the so-called ‘deep web’, which escape measurement.
between the conventional institutional territories (e.g. States, towns, international and regional organisations). Second, the DS potentially gives rise to new territories.

New relationships with conventional or traditional institutional territories, formed as a consequence of the DS, are generated by the phenomenon of detachment from these territories. The DS creates new sets of circumstances, particularly those born out of the global digitisation process. Facts are seized by data. The collection, processing and movement of such data in dematerialised form create circumstances that are detached from the conventional territories. The data generates a value that is intangible and independent from the physical resource itself. Once this data moves around in its own sphere, it generates a new relationship with the traditional institutional territories.

The other perspective offered by the emergence of a new space is the emergence of new territories, distinct from the traditional institutional territories. The way in which the law has dealt with new territories in other existing spheres is a classic illustration of the lawyer’s ability to revisit their subject areas in line with developments in human ingenuity. There are many relevant illustrations of the law’s quest to cover human ingenuity with its constructions: the atmosphere and space laws in continual transformation, the hydrosphere and current discussions of regulation of the high seas, the lithosphere and the highly-debated case of the Arctic and even the biosphere and all of the legal constructions developed around natural resources, in particular food.

The sphere is, by definition, a space where the data circulates and gives birth to new relations to the territories. This phenomenon is one of the most striking contemporary manifestations of the digital activities.

In the present paper, we consider data in three different states. First, data at rest, that is the issue of the legal qualification of data, its location for storage and the consequences of its location. Second, data in motion, which is data

---

7 One might think that most of the data reaching the DS originates from urban areas. This is far from being the case. In fact, the cultivated areas, although sparsely populated, are becoming increasingly connected to the DS. See S. Grumbach, 2015. ‘Big Data and Agriculture, From bytes to crops and conversely’. Operational Database Management Systems. Retrieved 27 February 2018 http://www.odbms.org/2015/07/big-data-and-agriculture-from-bytes-to-crops-and-conversely/. To this, one can add all the meteorological data, those collected from the seas and oceans, and all those which allow us to discover outer-space.

moving from one node of the network to another, potentially being aggregated with other data. Third, *data in action*, which concerns the exchange of data in support of some action in the physical world.\(^9\) For each state, we consider the conflicts arising and the legal solutions proposed in different regions. Reflections on governance issues are mainly related to data in action. The juxtaposition of the three states is also interesting; they constitute the three main pillars of the data regulation with a lot of interactions between each other.

2 **Data at Rest, Objects of Economic and Legal Relations**

In the DS the elements that comprise it are not natural (i.e. they do not exist in nature and simply have to be found, collected, and organised). The elements of the DS are of a digital nature and therefore must undergo processing. The remark, although obvious, reminds us of the importance of common standards which allow data to be understood, aggregated, extracted and processed. The obvious example is that of data that were formed and used in the first ages of digital equipment and that are now practically useless, unless they are converted in contemporary formats, at some cost.

This technological dimension implies that one must take into account evolution, obsolescence and interoperability. Data can and will increasingly fall into disuse and decay, and will be discarded. ‘Data archaeologists’ will search and investigate it, but this is of limited importance for the functioning of the DS. At the same time ‘data archives’ are an essential feature of the DS, especially in an already near future in which it will no longer be convenient to access them.

Therefore, if the DS is composed (also) of data, which require an act of conversion into new format, it is useful to start establishing a taxonomy of the kinds of data according to the way they have been created.

2.1 **Datafication of Real Life Objects**

The datafication of real life objects has until now been one of the most common ways through which data is created. A printed book is scanned, the digital photograph of an object is taken, the sound of an event (whether a conversation, a musical event, a natural phenomenon) is recorded, etc. Roughly

---

speaking, one can imagine that through this process the whole material world is, or can be, datafied, creating a parallel digital world. A good example of such duplicity is the Google Street View service which offers a reproduction, from many different perspectives, of a town. Although in some cases it is intended to work as a map, the amount of information contained in the data goes well beyond simple directions and virtually transports the viewer to that specific spot.¹⁰

The digitalisation of objects, although far from being completed, concerns a duplication of the real world, which is one of the features of the DS – a duplicate that can be used anytime and anywhere by an unlimited number of people, adapted to one’s needs or interests, and transformed in something new and different.

Seeing things from outside of the DS this means that objects in the material world, once datafied, have what might be considered a ‘second life’, and the two ‘spaces’ constantly refer to one another. Additionally, although digital versions of material objects (e.g. of a book, of a painting, of a musical performance) have existed for decades, putting them in a broader environment of interaction with other data illustrates their complexities, and also their significant differences, once one considers the DS.

There is a further aspect that must be stressed: while in the physical world of objects, animals, humans, the environment changes every second, the DS is able to register and recall every evolution. A person dies in the physical world, but not in the DS, which may preserve forever all of his or her data and even artificially continue to live.¹¹ The ‘T’ factor is one of one of the distinctive features of the DS, because it allows us to constantly add a fourth dimension to the knowledge of the world.

However, beyond the ontology of the DS there are economic and legal consequences. The value of an object is enhanced in the DS. In some cases, an object might have a value only, or mainly, because it is part of the DS and can be subject to a multiplicity of uses. The DS is therefore *per se* an economic phenomenon inasmuch as it creates, increases or transfers value.

---


From a macro-economic perspective one could ask oneself: what is the overall value of the DS, and what is its relevance and impact on the GDP of a country or of a region? Again, what appears useful is to consider it as a whole. Oversimplifying the entire 'sphere' is much more valuable than the sum of its single components.

2.2 Datafication of Information

Another way of creating data which pertains to the DS is by creating, from its origin, data. Its origin is the representation of non-material entities: news, information, results of research, etc. Being non-material they do not exist beyond the intellectual sphere. They are brought into existence through digitalisation, just as this paper that did not exist before being put into a file.

The difference in respect to the first case we examined (the datafication of real life objects) is that in the former case the creative moment arises when the object is digitalised, whereas in the latter, it coincides instead, more or less, with the moment in which the entity exists; it does not have a double nature – material and digital.

Because this is the ordinary way through which non material entities are now created, this could mean that they are subtracted from the material world, where, before the digital age, they existed if they were embodied in a material object: a book, a newspaper, a film reel, a vinyl record. This process is well-known and over the last three decades has generally become to be known as 'de-materialisation'.

From this point of view the DS is not a duplication, as with the previous case. Rather, it is entirely novel and generally has only one 'life', although this is extremely dynamic. What is clear is that when we have an entity that is 'genetically' digital, its nature does not relate to the material world and does not change in accordance with what happens in that world (e.g. the digital image of a monument that in the meantime has been destroyed).

Also in this case we have economic, and therefore legal, implications. Entities which are expressed only (or nearly exclusively) in a digital form create a barrier for the 'digitally illiterate' or for those who do not possess the adequate skills to apprehend such data. This, on the one hand, can reduce the value of data (typically when it is in a uncommon format); but on the other hand it shows us that the DS can be exclusionary and that those who have access to it do not necessarily coincide with the whole population, let alone humankind. Therefore, while digital technologies can surely be inclusive and broadening, they can also determine the opposite effect. Furthermore, as the DS has its 'rules', the lack of knowledge regarding how to access it and operate on it constitutes a further barrier.
2.3  **Datification of Persons**

Persons are nearly entirely digitalised, or datafied. Not only is most of the information on their activities, past and present, stored somewhere in a digital form, but their physical elements, both external and internal, are also registered, collected and processed.

The first aspect pertains to all the activities humans perform and which are registered through digital technologies. The most obvious are those activities which are done while connected to public telecommunication networks, but also included are all activities performed on restricted networks, such as payment systems, workplace or domestic networks. To these data one must add those which are collected through Internet of things (IoT) devices or through wearables. At the same time, all our physical features are datafied: security controls in airports, digitalised medical records held by national health services, DNA banks for medical, police or administrative reasons.

This duplication will increase even more with personalised artificial intelligence systems which will be able to replicate, on the basis of the data provided, the behaviour of single individuals.

2.4  **Automatically Generated Data**

An evolution of the previous case is that of data which is generated automatically by digital technologies. Until recently the main procedure was the use, by humans, of apparatuses – computers, mobile phones, payment devices etc. – connected to a telecommunication network which recorded the data concerning the activity, both in terms of connection and of content. The immense volume of data produced, mostly via the Internet, has allowed the so-called ‘Big Data Revolution’.

The first aspect that must be stressed is that these data – which powerfully fuel the DS – are automatically created, even without a wilful decision of the user. And while in the previous case there was a certain amount of creative work behind the datification of non-material entities, in this case the process is strongly enhanced by the system, which is structured in such a way as to extract, permanently, the greatest possible amount of data from each access to the DS (a typical example is that of trackers as well as so-called cookies).

This data is engineered in such a way as to be able to be combined with other data and appropriately processed in order to extract certain information. The way in which data is generated also raises issues concerning its ownership: the most recurrent case is that of someone wanting to delete the entire contents of an e-mail account, but being unable to eliminate all the meta-data which is (jealously) held by the service provider.
The process of self-generation of data is dramatically advanced by the increasing deployment of so-called IoT technologies, where objects collect and transfer data concerning their whereabouts, their functioning and the context in which they are placed. This already happens regularly with a considerable number of highly technological (and valuable) objects (e.g., luxury cars) but is gradually being extended to most household appliances as well as industrial and production structures. The deployment of IoT technologies is seen as a powerful boost for agriculture and agricultural products, especially those that have a very short consumption period and which must be under strict sanitary control (from fresh milk to oysters). The widespread use of IoT technologies in consumer goods is foreseen in the near future.

The difference between the first kind of self-generated data and that arising from IoT is quite obvious: in the first case, it concerns human activity which is done through a telecommunication network. It is therefore entirely virtual. With IoT, the data which is generated concerns a physical object belonging to the material world, and eventually its relations to humans.

The sheer volume of such data is included with velocity in the DS, which thus increasingly provides—or attempts to provide—an accurate and real-time representation of the whole world. However, metaphorically, we are very far from the primitive example of a global mirror that reflects what is going on in the real world. The DS is a substantial part of the world; it constantly interacts with it, and, to a certain extent, can even be autonomous from it.

There is a further element to be considered, which has both a social and an economic impact: IoT records the ‘life’ of the object. Until now, objects were mostly silent as to their ‘history’ with the exception of some very special ones, such as ships and aircrafts. Now this is also becoming a common feature for millions, even billions of objects. Not only will it be much easier to write, in the future, about what is called the ‘histoire de la culture materielle’, but it will also be possible to establish the value of many objects by looking at the data that has been recorded: now a bus, tomorrow, houses and buildings.

Again, one must stress the time dimension of the DS, which will be stratified with regards to the past and used to forecast the future. Conclusively, analysing the different ways through which the DS is filled gives us an idea of its nature, dimensions and evolution.

2.5 Forms of Appropriation of Data

Once one has established the DS as an autonomous space of which data is the main component, it is important to examine how the data within it is appropriated, controlled and managed. The difference with the material world is obvious inasmuch as we had, at its origins, immense and uncontrolled spaces
and things, which have been gradually occupied by humans. With the DS, from the very start, the data refers and is referable, according to its forms of creation, to some entity. We are not facing, therefore, a saga similar to that of the conquest of the West, or science-fiction colonisation of outer-space.

The development of the DS therefore is not about the discovery of new spaces, but rather about the building of a sphere in which – as with urban planning – everything has a specific ‘tag’ on it identifying its nature, structure, use and entitlement, and the relations that are developed in such a sphere.12

2.5.1 Seclusion of Data
The first aspect that must be considered is that of data that the ‘creator’ has secluded within the DS. It exists, it surely partakes of the DS, but only one entity – or those that have been specifically authorised – may use it and extract utility from it. This not only is the case for business data that falls under the notion of a trade secret,13 but also with regard to a great number of data held by public bodies which, for obvious reasons, are not available outside a very restricted group (e.g. police, military and security data).14 In the DS, therefore, there are a certain number of ‘closed spaces’ that are excluded from introspection and do not enter – unless the holder specifically decides so – into relation with other data.

Its value – not only from an economic perspective – is ensured by this policy. Data in the information society has a strategic value and although one is used to considering it to be what economists call a ‘public good’ (non-consumable and non-rivalrous), quite often the aim is that of ‘hoarding’ the greatest amount of data, possibly preventing third parties from sharing or recreating it. This shows that in the DS there are very clear relations of power (political, military, economic, and social) in which data play a similar role that wealth, natural resources and arsenals play in the material world.

---


14 See the exceptions set out in Article 1, letter (a) and (c) of Directive 2003/98 of the European Parliament and of the Council (as amended by Directive 2013/37) of 217 November 2003 on the re-use of public sector information [2013] OJEU L-345/90.
The DS is not, therefore, some utopian environment, but partakes, for better and for worse, in all the aspects of humankind.

2.5.2 Technical Protection of Data

The DS is a technological space, and data are the product of digital technology. Setting apart data that is – and is meant to be – secluded, the control of data passes through technological means which have manifold purposes, for example guaranteeing its authenticity, avoiding its alteration, enabling it to be properly processed and joined with other data, tracking its ‘movements’ etc.

The DS is essentially dynamic, not only because it is based on an ever increasing communication network, but also because the change of paradigm which brought the development of the DS is the result of a continuous circulation, inter-change and the creation of data. The protection of data is therefore essential in order to ensure the functioning of the DS. By asserting control by the ‘owner’ of the data, not only the individual objective of control is ensured, but also a general ‘social order’ of the DS.

As we shall see, the DS is eminently governed by technical rules, and as a matter of fact it presents in an extremely condensed way a feature that is typical of contemporary societies – that of being governed by technical rules embedded in the activity or in the product. In the case of the DS the well-known axiom ‘code is the law’ (where ‘code’ means the binary code) is dominant. This entails important aspects concerning the governance of the DS; the question of whether there can be a ‘democratic’ DS and what its features would be; and what the consequences of shifting decision-making processes to a class of technologists are. The DS is therefore – as any other human context – a political environment that requires constant critical analysis.

2.5.3 Legal Protection of Data

The dominance of technological aspects does not prevent the DS from being exposed to legal rules. The list is extremely long and ranges from protection from unauthorised access to data to data-theft; from personal data protection to data-banks; from intellectual property rights on computer software and algorithms to patents on production and business processes; and from digital identity to electronic voting systems. The complex relationship between digital technologies and the law has been widely studied over the last half-century and lawyers have long organised a ‘digital sectorial legal system’, classifying its various aspects and trying to fit the various kinds of data and the relations they create into legal categories.

---

The challenge with the DS is to set aside an isolationist approach in which each area of knowledge creates its own system scarcely in relation with other, essential aspects. The DS is, and must be considered as, a whole. Each aspect interacts, influences and is influenced by the others. Clearly legal aspects play, or can play, an important role in the protection of data and in the orderly functioning of the DS. One should, however, constantly take into account the effectiveness of legal norms, and to what extent their place is taken by technical solutions (which hypothetically might even be *praeter legem*), which impose themselves with a much higher level of compliance. From this point of view one should always keep in mind that legal norms have an ordering function, in the sense that norms are meant to shape society and relations within it, and/or to consolidate and justify existing patterns. Conflicts, claims and the need for adjudication are generally the pathology of a norm. It is therefore necessary to examine *in concreto*, even in the DS, the actual role of every norm.

2.6 ‘Ownership’ of Data

Although we are already immersed in a world of data, and despite the immense wealth that is already extracted from them, there is a considerable uncertainty regarding an essential aspect of any developed society, i.e. what one can call the ‘ownership of data’.

This aspect is fundamental for the orderly functioning of the DS, just as ownership of material objects (from land, to natural resources, to movables) is for the traditional world.

2.6.1 Civil Law Model vs Common Law Model

The uncertainty is the result of two converging problems:

- Traditionally there are two models of ownership which have developed in the Western world, and that result in different ways of organising legal

---

The ‘Datasphere’, Data Flows beyond Control & the Challenges

Relations.17 On the one hand we have the Roman law tradition (which has evolved into what is called now the civil-law tradition and which covers continental Europe and Latin America), in which ownership is deeply rooted in the material possession of a physical object, which gives rise to exclusive entitlement. The owner is therefore the legal entity that can exert on this material object a host of legally protected rights, qualified as ‘property’, whose content is generally summed up by age-old Latin maxims such as *ius utendi et abutendi* (the right to use and abuse) and *ius excludendi alios* (the right to exclude others).

On the other hand, we have the common law tradition, which from medieval England has subsequently expanded in former British colonies: the United States, Canada, Australia, and New Zealand. The common law approach is much more abstract inasmuch as ‘property’ is not (only) the legal relation between the entitled entity and a material object, but practically all the legal relations of economic value between private parties.18 This includes any utility (e.g. a credit), including future ones. The common law notion of property, because it does not need to have a material object to which it must refer, has been able to adapt itself much more easily in an economic context in which, over the last 70 years, wealth has moved from goods to services, and further to de-materialised relations.19 From a practical point of view this means that while in many civil law jurisdictions it not possible – even theoretically – to exert full-fledged property rights over data because they are not physically tangible (a typical example is Article 90 of the German BGB: ‘Things in the legal sense are corporeal objects’), there is no theoretical obstacle to claiming a ‘property right’ (in the common law sense) on data. It obviously remains to be seen what the extent of such a ‘right’ is, i.e. which remedies the holder has against those who have violated such a right.

Although what has just been said might point out a superiority of the common law approach in the DS, and also explains, in part, why the DS has developed so rapidly in a common law country such as the US, one should be cautioned from jumping to conclusions by considering that historically all

---

18 This aspect is investigated in Chapter 3 of U. Mattei, *Basic Principles of Property Law: A Comparative Legal and Economic Introduction* (Greenwood Press, 2000) 51 ff, where the economic efficiency of the two models is compared.
19 Already in the 1960s the term ‘new property’ was coined in the US and referred, mostly, to the entitlements of individuals vis-à-vis public institutions: see C.A. Reich, ‘The New Property’, *Yale Law Journal* 74 (1964) 733.
Western legal systems have always been at pains to cope with legal relations concerning non-material entities. The best example comes from one of the key tools of the DS – computer software. In the 1960’s, the United States of America (US) Patent Office rejected the claim that software could be patented, and therefore, after an intense lobbying by software producers (at that time the main producer was IBM), the 1980 Computer Software Act was passed by Congress. It took European countries nearly a decade to adopt similar laws. At any rate, the history of the protection of software shows that when a new entity becomes of wide economic importance, a legislative intervention (and not simply general practices of the trade) is required, which establishes who is entitled to use it, under what conditions, for how long, and what the exceptions to the general rule are.

With regards to data – and therefore to the DS – these interventions are only very partial and concern only certain kinds of data, or the way they are organised. This limited framework and the fact that there are significant differences in approach between the US and the European Union clearly do not help a harmonious development of the DS which, it is assumed, is global and loses its importance and overall value if it is fragmented across many small spaces that are each governed by their own set of rules.


21 For this reason the appropriate term, rather than ‘property’ or ‘ownership’, appears to be ‘entitlement’: see Van Erp (n 16): ‘This does not mean that no primary right (in the sense of the maximum of powers, rights, privileges and immunities) exists, but it is not ownership, but entitlement.’


23 Some authors speak of a ‘Balkanization of the Internet into multiple, closed-off systems protected from the extraterritorial reach of foreign-based ISPs’ (J. Daskal, ‘The
2.6.2 **US Approach vs European Approach**

Having outlined the two competing models, it is also important to state an obvious (at least to lawyers) point: any law pertaining to economic activities has a regulatory function and apportions wealth according to expressed or implicit policies. In the DS things are not different, and the rules that apply to data and the technological tools used to organise and extract value from them are in no way different.

One can easily compare two models, which correspond to two different approaches.

- The US approach, since the Computer Software Act, has been extremely protective towards all inventive and business activities in the field of digital technologies, which are protected by that Act but also by subsequent laws on semiconductor chips, and very strong – in the sense of rigorously enforced – patents on the various components of the hardware.\(^\text{24}\) However, the main resource of the DS, i.e. data, has been left much more free to be appropriated, especially personal data. Therefore, DS enterprises have been able to collect – with very few substantial limitations and at a very low cost – the main ‘raw material’ they use. This approach is not novel. In the first stages of the industrial revolution, factories were allowed to use water (whether from rivers, lakes or from underground sources) at no cost. From an economic point of view the policy is simple: DS industries receive a substantial incentive to develop new digital technologies, concentrating their efforts on how to collect and process data without having great concerns regarding the cost of the latter. This approach has been incredibly successful: US data companies have become world leaders and every day are offering new models, new tools and new products to the market.

The European approach is considerably different. Not only is the general approach much less ‘free market’ than that of the US, but Europe also has a historical legacy which it cannot shake off. Since the Enlightenment it has been commonly perceived that the role of government – no matter what the political regime is (absolute Monarchy, democratic rule, or dictatorship) – is that of deeply regulating industry and business activities which must comply with general welfare policies. The whole European welfare system – which inspires labour laws, social security, taxation – has the effect of burdening enterprises with direct and indirect (typically compliance) costs that their US counterparts do not bear. From this perspective, data – and especially personal data – are not a freely obtainable ‘raw material’. Data protection laws, seen from an economic point of view, restrict access to this resource, in some cases entirely removing it from the market (typically medical data, which in the US are usually traded instead),\(^{25}\) or increasing the administrative costs of collection and processing. Clearly, this results in a much less ‘friendly’ environment for DS enterprises and explains, in part, why Europe has no great data companies.

The comparison between the two approaches highlights again the politics of the DS. Does one prefer more innovation (albeit ‘destructive’), the development of new enterprises and the creation of new sources of wealth, which, at the end of the day, should profit most members of the community? Or is a much more controlled environment in which individual rights and general welfare play an important and countervailing role preferable? In democratic regimes these choices are normally made by voters, but if the DS is meant to be

global one easily understands that the politics of the DS are also international politics between great powers.

2.7 Personal Data

Among one of the most relevant components of DS are ‘personal data’, which are subject to extensive regulation not only in Europe but also in the rest of the Western world. Theoretically, one could imagine that by setting rules on personal data one could (or should be able to) govern the DS.

The first question that comes to the mind of a European continental lawyer is whether a person owns his/her data. This brings us to analyse how, in those legal systems, at the beginning of the 19th Century, the category of ‘personality rights’ (name, reputation, image) started emerging. When the first data protection laws were enacted during the 1970’s and 1980’s, it appeared natural for continental lawyers to place ‘personal data’ among personality rights.

However, as one does not ‘own’ one’s name, one does not own entities even more impalpable, such as ‘personal data’. One is reminded of Ulpian’s golden maxim: ‘Dominus nemo membrorum suorum videtur’ (‘Nobody is the owner of one’s limbs’). What the law confers upon individuals is the right to exclusive use and exploitation, and a series of remedies for unauthorised use and for injury.

The difficulty of applying traditional ownership models is evident considering that any digital entity – which is naturally composed of data – can be reproduced without limits, rendering the idea of exclusivity modelled on the property of tangible objects quite an illusion. Over the last 40 years, data protection laws have become increasingly complex. The General Data Protection

---

26 This is the definition provided by article 4 of the EU General Data Protection Regulation (n 22): “personal data” means any information relating to an identified or identifiable natural person (“data subject”); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.


28 Again this brings us to use, also in the field of personal data, the more appropriate term of ‘entitlement’: see footnote 21 above.

Regulation (GDPR) and its various annexed pieces of legislation comprise over 200 articles,\(^{30}\) of growing complexity.\(^{31}\)

Whatever may be the faint relationship with the traditional category of “personality rights”, it is clear that once personal data enter the DS they are mingled and mixed with zettabytes of other data making it practically impossible to track and control them. Metaphorically, it is as if law of the sea were based on the principle of controlling every drop of water in the oceans according to its origin.

Surely individuals dispose only of a nominal entitlement, which is very cumbersome to enforce, because it may, hypothetically, be possible to trace one of the many entities which process their data, but it is impossible to discover the

---


31 The implications of this normative over-growth have been clearly and convincingly set out by B.-J. Koops, ‘The Trouble with European Data Protection Law’, Tilburg Law School Legal Studies Research Paper Series No. 04/2015. Retrieved 28 February 2018 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2505692. The abstract is sufficiently explicit: ‘The trouble with Harry, in Alfred Hitchcock’s 1955 movie, is that he’s dead, and everyone seems to have a different idea of what needs to be done with his body. The trouble with European data protection law is the same. In several crucial respects, data protection law is currently a dead letter. The current legal reform will fail to revive it, since its three main objectives are based on fallacies. The first fallacy is the delusion that data protection law can give individuals control over their data, which it cannot. The second is the misconception that the reform simplifies the law, while in fact it makes compliance even more complex. The third is the assumption that data protection law should be comprehensive, which stretches data protection to the point of breaking and makes it meaningless law in the books. Unless data protection reform starts looking in other directions – going back to basics, playing other regulatory tunes on different instruments in other legal areas, and revitalizing the spirit of data protection by stimulating best practices – data protection will remain dead. Or, worse perhaps, a zombie.’
hundreds of other databases in which they have been transferred and in which they are used. It is therefore much more realistic to investigate the role of large entities, in the first place public bodies, that can exert a control over the bulk of personal data they collect and manage. But what is at stake in these cases is not ‘ownership’ but a legally conferred right to collect, process and use that data.

Seen from the perspective of the DS, the continental European model is put to task, because whatever the nature of the rights that individuals may have over their data, their enforceability appears to be, in most cases, illusory. Furthermore, the European model must compete with other powerful models including, first of all, the US one that, in practice, favours the extraction, by giant data companies, of the maximum of value from personal data. Therefore, one is not concerned so much with data belonging to individuals but with vast databases which are among the main components of the DS. This approach appears to be much more appealing in those far-eastern systems where the founding block is not that of individual rights but rather that of the general interest of the community.32 The ‘personal data’ model therefore appears to shrink in size, numerically and geographically.

The question, therefore, is whether in the DS certain traditional partitions of the law are still appropriate and functional, or whether it is necessary to adopt a different, more dynamic view, also towards personal data seen in action and in interaction.

2.8 Location of Data and Applicable Law

From what has previously been said it is clear that the location of where the data is stored has a significant impact on both the conceptual framework and the specific applicable law. One does not want to enter into lengthy private international law issues (which are already amply examined by legal doctrine),33 but simply illustrate some competing perspectives. One should, however, immediately add that in many cases the conflict will not be between private laws but between different claims by public law to control the matter.


In the first place, one might imagine that data, being immaterial, is legally attached to the entity that retrieves, stores, processes and disseminates such data. This brings us to the place of establishment of the entity, a line which was, creatively, introduced by the Court of Justice of the European Union in the Google Spain case in order to apply – contrary to most precedents – EU data protection law to data related to the Spanish subsidiary of Google.\footnote{For some comments concerning the issue of whether it could be said – as the Court of Justice of the European Union (CJEU) said – that Google had ‘stable arrangements’ in Spain, see I. Spiecker Dohmann, ‘A New Framework for Information Markets: Google Spain’, Common Market Law Review 52 (2015) 1033; extremely critical G. Caggiano, ‘L’interpretazione del criterio di collegamento del “contesto delle attività di stabilimento” dei responsabili del trattamento dei dati personali’, in: G. Resta and V. Zeno-Zencovich (eds), Il diritto all’oblio su Internet dopo la sentenza Google Spain (Roma TrE-Press, 2015) 43; and P. Piroddi, ‘Profili internazionalprivatistici della responsabilità del gestore di un motore di ricerca per il trattamento di dati personali’, in: G. Resta and V. Zeno-Zencovich (eds), Il diritto all’oblio su Internet dopo la sentenza Google Spain (Roma TrE-Press, 2015) 63 (available open access).} In the DS, however, there might be multiple entities involved, creating considerable confusion as to who, actually, is holding the data.

A second approach would be that of establishing where, materially, the activity of collecting and processing is actually performed. One might object that this is an extremely fuzzy notion, especially if one looks at so-called cloud computing. However, this is exactly the reason why it could be extremely appealing to States wishing to assert their jurisdiction over the data, using extremely vague technical references which enable it to claim that those data are on the territory of that State and therefore fall under its laws.\footnote{The opposing views are clearly presented in the In re Microsoft case decided, in the first instance, in the sense that US federal authorities could order Microsoft to hand over data held in Ireland [15 F. Supp. 3rd 466 (S.D.N.Y 2014)], but reversed on appeal by the Second Circuit [15 F. Supp. 3rd 466 (S.D.N.Y 2014)] (there was no intention of Congress to give courts extraterritorial jurisdiction over data stored overseas, and thus, the district court lacked jurisdiction to enforce the search warrant on Microsoft for customer data stored in Ireland). For some of the many issues surrounding ‘digital sovereignty’, see V. Zeno-Zencovich, ‘Around the CJEU Schrems Decision: Digital Sovereignty and International Governance of Telecommunication Networks’. Retrieved 27 February 2018 https://ssrn.com/abstract=2788789.}

A third approach – more nuancé – would be that of distinguishing between the multiple reasons for which a jurisdiction is called upon to establish rules for the governance of the DS.
From this perspective, criminal, administrative and private law cases are different from each other and might suggest different solutions, and one might break down the latter segment: are we talking of ownership rights over portions of the DS? Or of the applicable law to the contract of sale or lease of data, or of the license to use them? Or is someone claiming damages brought by the data or by their improper or negligent use?

The sheer size of the DS poses, from a theoretical perspective, issues and doubts that are recurrent when trying to provide a legal governance of outer space, and confirms the risk that each State will attempt to claim that it has jurisdiction over the DS.36

3 Data in Motion

We propose to demonstrate the importance of data flows by a progressive, explanatory approach to the phenomenon, considered in its generality in a casuistic, legal, comparative and governance way. We consider it from the point of its most extreme manifestation through to the hypothesis of a total circulation of data beyond control whose legal validity and utility will be questioned.

3.1 The Phenomenon of Data Flow: A Casuistic Approach

Let us begin with a few examples of everyday life. A person posts data on their blog. They decide an hour afterwards to withdraw them. In the meantime, the information has been indexed by search engines. The data continues to be accessible on the Internet even if over time it is necessary to go deeper in the indexed pages to find it. We receive lots of emails every day. Several times a day, we redirect mails, and so do our correspondents. These data move from servers to servers for storage and treatment, without our knowledge.

A person using a mobile phone to find the precise address of a store, when entering the store, might receive a message by email proposing a promotional offer, although they do not remember having been customer of this store, nor having communicated their email address. We de facto fill in forms every day on the Internet, without having any idea of the geographic location where the data is stored, or even the identity and location of the people who can access it.

Let us now turn to international news. 37 Denmark has purchased mass data from the Panama Papers to combat tax evasion on its territory. 38 The Yahoo group announced that 500 million user accounts have been pirated. 39 The Telegram App did everything possible to protect itself from state surveillance. 40 WhatsApp (an App bought by Facebook) announces the sharing of data concerning its users with the social network, triggering the reaction of the G29 European data protection group. 41 A massive espionage of confidential information on French Scorpene submarines was revealed in Australia. 42

The list of such examples is unbounded, and the phenomenon will only accelerate with the considerable multiplication of objects of all kinds connected to the Internet and the massive use of the data thus collected by social networks in particular.

3.2 First Legal Approaches at the European, National and International Levels

The law is concerned with the question of the circulation of data in terms of the definition of the legal conditions of this circulation. A brief comparative overview suggests the following major elements at the European, national and international levels:

37 We limit ourselves to news disseminated by the press over a recent and short period (Fall 2016).
• the general European Union system for the protection of personal data carries a very high ambition to regulate the flow of data;\textsuperscript{43}
• The specific national civil or criminal penalties for data leakage: the legal bases vary considerably from one area to another, depending on the nature of the data, the justification of its confidentiality or control;\textsuperscript{44}

The cross-border circulation of data poses specific problems of international law: public international law, whether to regulate these flows by international agreements or unilateral decisions of international scope (examples of decisions taken regarding transfer/sharing Transatlantic data: PNR,\textsuperscript{45} Safe Harbour,\textsuperscript{46} Privacy Shield);\textsuperscript{47} private international law (determination of the

\textsuperscript{43} See in particular the General Data Protection Regulation (n 22) and compare it with the French ‘Loi n° 2016–1321 du 7 octobre 2016 pour une République numérique’ (Law for a Digital Republic) whose Part I is entitled: ‘The circulation of data and of knowledge’.


\textsuperscript{45} Circulation of PNRs is now regulated by Directive 2016/681 (n 30). The EU has signed bilateral PNR Agreements with the United States, Canada and Australia. On the transfer of financial messaging data see the 28.6.2010 “Agreement between the European Union and the United States of America on the processing and transfer of Financial Messaging data from the European Union to the United States for the purposes of the Terrorist Finance Tracking Program” (published in the OJEU L 195 of 27.7.2010). The envisaged agreement with Canada on the exchange of PNRs has been challenged in front of the CJEU (Case C-1/15 European Commission v Republic of Austria). The decision pursuant article 218 TFEU has been delivered on 26.7.2017. Following the opinion of A.G. Mengozzi, it indicates a long list of provisions that are not deemed compatible with the European Charter of Fundamental Rights, and an equally long list of provisions that require significant amendments.

\textsuperscript{46} The Commission Decision 2000/520 of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce OJEU L 215 was adopted by the Commission on the legal basis of Article 25(6) of Directive 95/46 to allow the transfer of personal data from Europe to US, which was considered to be a ‘safe harbor’. This decision was voided by the European Court of Justice (ECJ) in the famous Schrems case (ECJ Case C-362/14 Maximillian Schrems v Data Protection Commissioner [2015] EU:C:2015:650) in consideration of the lack of protection of personal data in US.

\textsuperscript{47} See the Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S [2016] OJEU L 207/1. Privacy Shield. For a comparison of the US and EU systems in this field, see notably D. Svantesson and D. Kloza (eds),
law applicable to the data circulating and the competent judge to settle any dispute relating thereto), transnational law (the current joint ELI-ALI feasibility study on ‘Principles for a Data Economy’).

3.3 **Total Circulation of Data beyond Control: Hypotheses for Comparative Law**

The total circulation beyond the control of data is a phenomenon of great amplitude, which may be of a nature to grasp the law in its most varied constructions.

In an essentially exploratory way, it is interesting to lay the groundwork for a reflection on the legal nature of the phenomenon that could be carried out from a comparative perspective in national, international and European law. Here are the first points:

- The phenomenon is rather a fact than a legal act essentially realised through a sequence of events (what lawyers call a legal fact) without their voluntary nature (what lawyers call a legal act) being required (since, by hypothesis, the circulation escapes the will of all actors);
- This phenomenon is necessarily complex – it involves stakeholders at different levels, all highly interdependent, with subtle retroactions, therefore relating to ‘complex systems’;
- It is mainly concerned with mass flows, whether directly or indirectly caused by humans’ activity, which attain their own autonomy. This approach by the existence of the mass questions the law. The legal regime of the mass could be different from the legal regime of the data, seen as single entities. It is certain that the legal treatment of the data in itself (according to its characteristics) does not exhaust the more general question of the legal regime of a mass of data. The treatment of mass can also be considered as such as a

---


50 For an analysis of the circulation of the credits through contract, see F. Carnelutti, ‘Teoria giuridica della circolazione’, (Padova: Cedam, 1933) especially at 72.
The ‘Datasphere’, Data Flows beyond Control & the Challenges

For example, the treatment of the mass of data by the ‘big data’ perspective could coexist with the legal treatment of the individual data. The situation is the same with the approach of the mass of data by the ‘common good’ concept (as air, water, high sea, etc.), which could cohabit with the question of the ownership of an individual data. The treatment of mass can also be considered as such.

- This phenomenon has a value (economic approach). This value can be the support of transactions (contracts) and of an organisation (branch/network). In the ordinary course, it is considered that the movement of persons or goods falls within the legal category of services (any contract of transport is a service contract). This category does not refer immediately to traffic but to the legal act which organises it. It does not make it possible to account for the phenomenon that interests us here (by hypothesis, no contract governs total circulation beyond control). The question to be investigated then arises, as to whether it is useful to speak of goods. This hypothesis questions the nature of the property and therefore its legal regime: an immaterial good (res incorporales), an abandoned good (res derelictae), likely to receive the qualification of a common good (res communes).

- The phenomenon raises questions about the level of intervention required: individual or collective (both naturally but with a strong ascendant for collective intervention given the magnitude of the phenomenon) and especially private (each private agent deals with cases).

All of these issues can be addressed in very different legal environments. Questions on the legal nature of flows will be mainly considered at a national level. On these difficult subjects, which are closely linked to the categories of private law, it is difficult to reach a consensus at an international or European level. Questions relating to the existence of a new space, new relations to territories and possible common goods, are clearly relevant at the international level, but Europe often manages to define solutions before they even penetrate the spheres of international law. It is therefore important to rely on the dialectical game between international and European law to try to advance legal actions.\(^{51}\)

3.4 Total Circulation of Data beyond Control: Facing the Risks

Total circulation beyond control does not necessarily call for legal intervention. If one compares this circulation with natural circulation (natural circulation of solids, liquids, gases in the traditional spheres of earth sciences:

---

hydrosphere, lithosphere, atmosphere), the law can remain largely foreign to the phenomenon and intervene only in, for example, a tornado described as force majeure, a watercourse that alters a boundary, etc.

An important point of difference, however, is that the situations are not perfectly comparable. Data flow beyond control has a human origin, which cannot be treated as a natural phenomenon, for if it produces effects, humans may be held accountable.\(^52\) Of course, this phenomenon has a strong collective dimension (even if it does not exclude individual acts), but it does call for two possible levels of intervention. Indeed, the phenomenon of total circulation beyond control can be understood as:

- A risk that requires the involvement of risk management mechanisms. If the private mechanisms (internalisation and socialisation of risk by a simple internal calculation of costs and their assumption of responsibility) suffice to reduce it, then the law does not have to intervene. If not, public intervention is needed: sanctions/reparation (criminal law, civil law), socialisation/metallisation (compulsory insurance, creation of guarantee funds); risk management could justify hitherto unsuccessful policies on the taxation of data flows; all this presupposes a prior measurement of the risk, its characterisation and therefore, at the first level, the recognition and definition of the total circulation of data beyond control.

- While the risks of full movement beyond control of data can be observed, it appears to be what is called an ‘invisible risk’.\(^53\) One can apply to this phenomenon the reflections presented over the last 40 years on the existence of a new geological era – the Anthropocene\(^54\) – which would follow an existing era: the Holocene. Both are marked by circulation phenomena that largely escape the control of man. Therefore, a connection could be established between these analyses and the largely ignored question of the total circulation of data produced by man and extending beyond his control. Among

---


the aspects that should be attentively examined are those related to risk management of a global nature.\footnote{55}{The EU 2008/114 Directive of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection [2008] OJEU L-345/75 defines (at article 2) a ‘critical infrastructure’ as ‘asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions’. One could suggest that data should also fall within such a definition by extending the scope of Recital 19, according to which ‘Information sharing regarding ECIS should take place in an environment of trust and security. The sharing of information requires a relationship of trust such that companies and organisations know that their sensitive and confidential data will be sufficiently protected.’}

4 Data in Action

An exchange of data is often associated with an exchange in the physical world. This is clearly the case for activities carried on digital platforms by users seeking goods or services, supported in particular by e-commerce as well as service platforms, such as those offering access to facilities, for instance. Digital platforms are the main players of the DS – they ensure a role of increasing importance that impacts remotely on actions across territories. These actions not only have an economic impact; they also contribute to the enforcement of new norms, and as such contribute to new forms of governance. They also concentrate an increasing share of the data available over any territory.

4.1 Digital Platforms in Control of Essential Services

Digital platforms started to emerge as new actors in the mid 1990’s. The first platforms were search engines, which revolutionised the access to knowledge, and e-commerce platforms, which deeply affected selling modes, followed later by social networks, which transformed interactions between actors as well as access to, and the production of information. They offered extremely efficient and innovative solutions to traditional problems, such as finding information and connecting with others.

The main activity of platforms is to offer intermediation services in two-sided markets,\footnote{56}{J-C. Rochet and J. Tirole, ‘Platform Competition in Two Sided Markets’, Journal of the European Economic Association 1(4) (2003) 990.} that is markets with, on one side, producers of goods...
or services, and on the other side, their consumers. Platforms intermediate between producers and consumers and connect them. Apartment rentals or ride-hailing services constitute good examples of such applications. The interaction between both sides of a market and a platform is exclusively digital: they only exchange data such as identity or payment information through applications and online portals. Thus, platforms tend to be able to scale quickly.

The example of Uber, which defines itself as a data company and not a ride-hailing service provider, illustrates the independence of platforms from specific infrastructures.57 The company neither possesses cars nor hire drivers. Uber can easily target all markets throughout the world and abstract itself from a specific territory. Even if some platforms may rely on a heavier infrastructure to deliver goods (the examples are prepared food delivery services such as Foodora or Deliveroo) or to gather customers, for instance, all platforms rely on a set of digital procedures or algorithms which handle a problem most people face independently of the landscape of a specific territory. The numerous conflicts between platforms and local labour or business regulations, for instance, derive from this abstraction.58

Platforms are creating ecosystems. They increase their abstraction from specific constraints and provide basic services that can be used by third parties to offer their services. This is very close to what governments do by ensuring essential services, such as water, energy, communication, etc., to serve individuals as well as corporations and to develop other services. No assumption is made as to how the initial essential service is used. Even when platforms seem to target a specific market, they generate data that allow them to become basic infrastructures for the development of other services. Transportation applications, for example, possess data on traffic jam or the state of the roads, which are necessary to understand the flows of people throughout cities and optimise resources consumption or quality of life. As such, they have turned out to be at the same time necessary partners and potential opponents to local governments.

Platforms have become so widely used that they offer essential services without which our societies would hardly function anymore. They have so many users that the rules they impose on their favourite playing field shake

the course of world. The debates around labour laws or the role of platforms in surveillance programs are only two examples of their importance. In a way, platforms govern users. For instance, they influence who they connect with and the information they access, but their governance departs from the traditional state-based one as they do not rely on a heavy vertical bureaucracy and visible demonstrations of power. On the contrary, digital governance is based on almost invisible reticular data collection procedures and incentives.

Clearly, platforms have shifted governance. Everywhere, legacy actors try to take inspiration from them. Nonetheless, the respective role of platforms and legacy actors is yet under elaboration as proved by current conflicts and negotiation around the place of platforms. Different scenarios could be deployed at different places and we now try to depict them.

4.2 Platforms and States, Who Controls the Data?

To a certain extent, platforms rely on the same material as modern governments: data. Statistics is the art of modelling the ‘things of states’ with the appropriate mathematical tools in order to influence them. Statistics constitute an essential tool or modern governing. So are data, which feed statistics. Statistics allow a new political rationality based on norms. They define normal life expectancy, unemployment rates, etc. and influence political action to guide behaviours towards these norms. During the last two centuries, the capacity of governments to obtain precise knowledge of their population has regularly been upgraded, with increasingly detailed censuses and technological improvements, such as the digitisation of census in the 1940’s, for instance. The improvement in life quality and expectancy is a direct benefit of data collection and processing that support public health policies, for instance.

Two important trends characterise the evolution of data driven governments nowadays. Firstly, the decline of state supremacy in the control of data existing in its territory. The management of very detailed maps of the territory, augmented with all sorts of data on activities, economic, transportation, etc. and

including pictures, constitutes a good example of the rise of platforms in the knowledge of the activity of the territory of a temporal accuracy unmatched by governments.62 Their relative share of such data has thus declined continuously since the turn of the Millennium. Secondly, the increasing political request for transparency and accountability of government, which implies more openness of administration data, and continuous evaluation of public action. This constitutes a complete change in the principles of public data management, which were closed by design.

The globalisation of the world economy, which resulted from the implementation of the principles of a liberal economy, facilitated the movement of people, goods and capital. It gave increasing facilities to private corporations to expand globally, while decreasing the power of governments. The free movement of goods and capital encouraged governments to adopt local rules that compete at a global scale. Such a competition progressively changed the political balance between concrete factual data and abstract political principles.63 Numbers have acquired an increasing political legitimacy, at the same level as political principles, which lead various political scientists to speak about ‘governance by numbers’.64

The second trend, which is also calling for more data, is the desire to have more transparency and accountability of public action. Political systems of Western democracies, as well as other political systems, are under pressure from public opinion to increase efficiency and reliability in the political sphere. Pierre Rosanvallon speaks of ‘counter-democracy’, that is new forms of democratic powers, taking shape ‘in the age of distrust’.65 He distinguishes three counter-democratic powers: oversight, prevention and judgment, which

---

63 E. Ostrom, Governing the Commons (Cambridge: Cambridge University Press, 2015).
strongly rely on a new ‘utopia’ of transparency. Therefore, evaluating public policies and making public administration data open to the citizens are new political trends that governments have to take into account.\footnote{And for further issues see J. Collmann and S.A. Matei (eds) Ethical Reasoning in Big Data: An Exploratory Analysis (Cham: Springer, 2016).}

In July 2013, while the UK was organising the G8 meeting, a rather innovative open data charter was proposed and signed by all participants. Its ambition covers a large spectrum of simple objectives ranging from politics to economy, and from better governance to increased development opportunities. The charter is really ambitious when it asserts the principle of opening all data by default, apart from essentially three categories of data that need protection related to national security, privacy, or intellectual property issues.\footnote{The text of the Charter is available online. Retrieved 28 February 2018 https://opendatacharter.net/.} The charter has been followed by many decisions, at all level of governance, including directives of the European Commission.\footnote{See the Council Decision (EU) 2017/1842 of 9 October 2017 on the open data policy of the Council and the reuse of Council documents [2017] OJEU L.262/1.}

State surveillance programs are increasingly making use of platforms data, but this results in complex trade-offs.\footnote{A. Butler and F. Hidyegi, ‘From Snowden to Schrems: How the Surveillance Debate Has Impacted US-EU Relations and the Future of International Data Protection’, Seton Hall Journal of Diplomacy and International Relations 17 (1/2) (2015) 55.} American corporations tend to make efforts to prove that they are not giving data automatically to the surveillance system, as demonstrated by the various cases in which Apple was enjoined to provide access to an encrypted i-Phone. The trust they enjoy from foreign users, which constitute the large majority of their users, strongly depends on their demonstrative resistance to state requests. The request of US custom officials, at the beginning of the Trump administration, to access digital devices unlocked by their users while crossing the border\footnote{See Andy Greenberg, 2017. ‘A Guide to Getting Past Customs with your Digital Privacy Intact’. Wired, 12 February. Retrieved 28 February https://www.wired.com/2017/02/guide-getting-past-customs-digital-privacy-intact/.} will most probably lead to technological offerings allowing the device’s content to be emptied on the cloud before crossing the border to recover all the data, directly afterwards.

A tricky game is taking place between platforms and governments on the control over personal data, with subtle trade-offs related to national security and trust.
4.3Platforms as Normative Actors
Platforms maintain a direct link with their users and are a portal to services, users and data. The direct link is fundamental in order not to lose data to other parties. Size matters for platforms, whose value follows a law ‘à la Metcalfe’, with a quadratic dependency on the number of users. The more users a platform has, the more data it will get and the more attractive it will be, considering that it is able to handle a large amount of users. The necessity of possessing a huge population of users may explain why there is a dominant platform that emerges in each sector. Indeed, to fully be a gatekeeper, a platform benefits from an essentially monopolistic position. As a platform becomes monopolistic, it gains enormous power and may conflict with public administrations.

Especially when it concerns the relationship between a community and a territory, one can see the growing governance role of private platforms. The most obvious example is that of the many mobility platforms that suggest the fastest route to reach a certain destination or the choice between various means of transportation. The same can be said of those applications that suggest places, neighbourhoods or towns where it is more likely to find people with the same interests. The governance role is present not only in short-term individual decisions. Inasmuch as they build behavioural patterns, they have long term social effects, influencing future choices.

In this line of long-lasting influence one can find the impact that platforms have on housing, health-care and educational choices, or on individual financial investments. The reliability of the information that is offered, and which orients choices, is a result of the quality of the data processed and of the tools that are used in managing the DS.

4.4Predictive Administration
Traditionally, administrative decisions – which cover most individual and collective courses of action that must comply with some kind of regulation – are

---


taken on the basis of statistical data and with attempts to foresee the future, mostly through demographic trends.

Can data analytics, commonly used by enterprises, be applied to administration? In this case, data captured by platforms – typically a platform managed by a local authority, such as a municipality – is used to predict future developments and to tailor decisions to a quasi-individual level through what are called ‘granular norms’.73 One can easily detect the legal pitfalls of such a perspective.74 If one applies age-old principles of administrative procedures, participation of stakeholders in the decision-making process, transparency of data and methods used,75 strict ambit of public powers, and the principle of non-discrimination, it is possible to challenge each and every step of ‘predictive administration’.76 The example is useful to indicate how difficult it may be to adapt what appears as a natural functioning of the DS to a legal system which – for very good historical and practical reasons – is eminently formalistic and not ready (and willing) to be substituted by algorithmic decisions.77

Data have played an increasing role in public administration for governance since the generalisation of census and statistics two centuries ago.78 With the advent of digital platforms, governments are upgrading their facilities with the ambition not only of increasing efficiency, but also transparency and

74 ‘Data are representations of observations, objects, or other entities used as evidence’; ‘Across the sciences, social sciences, and the humanities, scholar create, use, analyse, and interpret data, often without agreeing on what those data are’ (C.L. Borgman, Big Data, Little Data, No Data: Scholarship in the Networked World (Cambridge: MIT Press, 2015) xvii ff).
accountability, as well as citizens’ participation. Meanwhile, digital platforms contribute to the enforcement of norms in an increasing number of essential aspects, such as labour, which conflict with laws in numerous countries.

Political power is partly a function of access to, control over, and the ability to work with data; the consequences of data flow imbalances could soon outweigh concerns about trade, capital account, and other traditional economic imbalances.

5 Conclusion

The law eventually adapts to new phenomena. Different approaches can compete to address them, such as the civil law model or the common law model, leading, for example, to orthogonal ownership principles. In the case of data, though, given the impact of systems making use of data on society, given the global, worldwide extent of these systems, given the tremendous flow of data they generate that is mostly beyond control and given the phenomenon of detachment, a radical shift of model may be necessary to be able to apprehend the new phenomena. We propose to use the notion of ‘Datasphere’ as a holistic concept inspired from earth sciences, which encompasses all data whatsoever, and globally models the activity as a complex system, taking into account interdependencies and retroactions. The DS allows us to consider a new space, and therefore new relationships with conventional or traditional institutional territories, as well as the emergence of new territories distinct from the traditional institutional territories. We have considered data in three states: at rest, in motion, and in action, corresponding to the three fundamental states of data in need of legal qualification and of governance. The differences between the various legal models might reflect an insufficient understanding of the new phenomena at play more than ideological choices. Clearly only the future will be able to tell us if this frame of reference is workable and can contribute towards a better comprehension of such a complex environment.