ANALYSIS
2016-09-06 Dnr 3.4.1-2016/00146-3

Utrikesdepartementet

Data flows – a fifth freedom for the internal market?

After years of heated discussions, the EU legislator finally adopted the Data Protection Regulation in 2016. This came after a string of dramatic developments affecting the free flow of data, from the invalidation of the EU rules on data retention to the rise of the right to be forgotten and the annulment of the Safe Harbour Agreement. At the core of these events is the tension between the fundamental right to privacy and the freedom of movement of data. This tension raises in turn the question of the status of this freedom in the internal market architecture.

The internal market is based on the freedoms of movement of goods, services, persons and capital. These four freedoms were introduced in the Treaty of Rome some 60 years ago, long before the emergence of the digital economy. Today our societies are increasingly dependent on the processing and transfer of data. Almost all transactions involve the movement of data at some point and our economies are relying on a smooth and free flow of data. At the same time, the EU legislator is taking actions that, in the name of privacy rights, curtail this flow. It is therefore legitimate to discuss whether the freedom of movement of data should be given stronger protection and even be upgraded as a fifth freedom.

It is in our view clear that the free flow of data constitutes a freedom of movement in its own right, distinct from the traditional four freedoms. It provides for a regulatory framework that harmonizes the rules on data in the EU. Those rules include many of the features that characterize the four freedoms such as the balancing of pro-integration arguments with legitimate interests, the removal of certain barriers to trade and the setting up of coordination mechanisms.

Yet, we find that the free movement of data differs from the four freedoms. First, it is an ancillary freedom in the sense that it lacks the primary law status of the rules on goods, services, persons and capital. In fact, the free movement of data is subordinated to other primary law rules, namely the fundamental rights of privacy and personal integrity. Second, the EU rules on data lack the maturity of the four freedoms. These rules are still struggling with fundamental issues such as the balancing of conflicting interests between data flows and data protection. This in turn affects the adequacy of the EU rules on data.

P.O.Box 6803, S-113 86 Stockholm, Sweden
Visiting address: Drottninggatan 89
Phone: 08-690 48 00, Fax: 08-30 67 59
E-mail: kommerskollegium@kommers.se www.kommers.se

We therefore note that there is a gap between the contribution of data flows to the functioning of the internal market and the way they are promoted in the internal market legislation. Firms and consumers increasingly use cloud services, online platforms and marketplaces to do business in the internal market (including the so called "sharing economy"). While data is currently allowed to be transferred freely within the EU, many such transactions in the internal market are enabled through storage and processing of data on servers located outside the EU. Therefore, barriers to the free movement of data to third countries may effectively constitute barriers to the freedom of movement of goods, services, capital and/or persons within the internal market. This relationship between the internal and external dimensions are confirmed by the CJEU[1] and strengthened in the newly adopted Data Protection Regulation.

However, while the freedom of movement of data deserves a stronger acknowledgment from the EU legislator, we do not see the need for an upgrade as a fifth freedom. Such an upgrade would not, in our view, alter its relationship to the fundamental right to privacy.

In addition, we view the flow of data as a malleable phenomenon. The dynamism of the digital economy is such that new technological developments and business models can accommodate the restrictions imposed by the EU legislator. As an example, only a few months after the invalidation of the Safe Harbour Agreement, new cloud solutions are devised to work out the general prohibition on the transfer of data to third countries. Much as other industries in the past, the market may be redefined, some players may disappear and the flow of data may be altered as a result of stricter privacy regulations but ultimately, and as long as there is a demand for it, it will continue supplying the economy with its "digital gold".

This does not mean that everything is fine and that the EU legislator should be given a *carte blanche* to restrict data flows in the name of data protection. Rather, legitimate concerns for the free flow of data should focus on ensuring that new privacy measures do not impose unnecessary restrictions. Just as the proportionality test applies in respect of the four freedoms, it is paramount to secure that EU legislation does not go further than what is strictly necessary for the protection of the fundamental rights of privacy and personal integrity.

Given the primacy of these rights, which in our view is not questionable, it is thus important to remain vigilant and remove any hinder that is not thoroughly motivated by privacy concerns. To take one example, there are in our view grounds to discuss whether such proper assessment was conducted in respect of the restrictive impact which the Data Protection Regulation may have on data flows.

[1] Case C-362/14 *Schrems*.

Table of contents

1 Introduction

The importance of the free flow of data for international trade and for the functioning of the internal market is obvious and has been so for several decades. More than twenty years ago, this was one of the main reasons for the adoption of the EU Directive on Data Protection (1995). The EU legislator emphasised in that Directive the key role played by the free flow of data for trade, both within the EU and globally.[2]

The Directive was in fact the last step in a process initiated in the early 1980s by the OECD and the Council of Europe.[3] Both organs were concerned with restrictions on the free flow of data resulting from differences in national rules on data protection. Interestingly, the general terms of the current debate between the free flow of data as an essential component to trade and the protection of personal data as a means to safeguard the rights to privacy and of personal integrity were already set almost four decades ago.

Another interesting observation to be made from the discussions of the 1980s and 1990s is that the free flow of data only became an issue for policy-makers to the extent that it was restricted by national rules on data protection. In other words, the concept of free flow of data developed as a response to the need to protect the rights to privacy and of personal integrity. It was defined in opposition to these rights and, therefore, both notions of data flow and data protection can be said to be intrinsically linked.

One main difference though between today's debate on the free flow of data and the discussions that took place in the 1980s and even the mid-1990s is the increasing dependency of our societies on the processing and transfer of data. The digitization of the economy means that very few transactions (if any) can be made without data crossing a border. This in turn means that it is more acute today than a few decades ago to preserve the free flow of data.

It is in that context that voices have been heard in the European debate calling for the recognition of the free flow of data as a "Fifth freedom". Reference here is of course made to the traditional four freedoms of goods, services, persons and capital which constitute the backbone of the internal market. Introducing a fifth freedom in the internal market architecture, its

---

[2] See for instance the preamble of the Directive: "*3.* [T]*he establishment and functioning of an internal market in which […] the free movement of goods, persons, services and capital is ensured require* […] *that personal data should be able to flow freely from one Member State to another …*" and "*56.* [C]*ross-border flows of personal data are necessary to the expansion of international trade*".

[3] See the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) and the Council of Europe Convention for the protection of individuals with regard to automatic processing of personal data (1981).

proponents would argue, is a means to reflect today's reality by taking into account recent, yet essential, means of economic integration.

The purpose of this paper is to discuss the role of the free flow of data as an instrument of European integration. In itself that flow carries the means to impact essential human rights, safeguarded by the treaty. Usually the legislator is satisfied by concluding that both data flows and human rights need protecting. However that is not always easily achieved. This paper sets out to set the framework for under which premises such a delicate act of balance should be carried out.

We note in that respect that there are numerous studies on the digitization of our economy, globally and in the EU, some of which focusing on the importance of data flows for economic integration. Although this is undeniably an important aspect of the issue, this report is mostly concerned with the place the freedom of movement of data, occupies in the legal and regulatory framework of the internal market. It provides for an overarching review of the current EU rules on data flows in relation to that framework and discusses the appropriateness of revisiting this relation.

This paper is structured as follows.

- In order to better understand the concept of free flow of data, we analyse first its main characteristics and particularly its contribution to trade (**Section 2**).
- This attempt at defining the free flow of data is supplemented with a review of the restrictions to the movement of data – a key element in understanding the scope of the free flow of data (**Section 3**).
- Given these two approaches, we examine in the following section how the free flow of data compares with the traditional freedoms of movement of goods, services, persons and capital. We find notably that the differences between the free movement of data and the existing four freedoms, in terms of maturity and standing, are in contrast to the importance of data flow for trade and economic integration in the EU (**Section 4**).
- This in turn raises the question – discussed in the last part of this report – of whether the free flow of data should be upgraded as a "Fifth freedom" within the EU regulatory framework (**Section 5**).

2 Identifying the need for the free flow of data – A positive approach

Data is the raw material of which information and knowledge is produced. As such, the importance of data is not a new phenomenon *per se* – early humans must surely have made inferences of how to best hunt for food (the information/knowledge) by processing and sorting various trial-and-error observations (the data) of previous hunting experiences. Fast-forward to today and the essence is still the same, but every aspect from observation, through collection, storage, aggregation, analysis and distribution, to final usage[4] of the data is vastly more sophisticated and powerful.

In the modern economy, data is a central factor in almost all types of business activities, partly as a facilitator of day-to-day operations but also in itself. Broadly speaking, this means that the increased possibilities for data collection and processing power have made "classic" business activities gone digital and subsequently online, while also creating entirely new types of activities that were previously unfeasible or unthinkable. An example of the former would be the way we can order a product, while an example of the latter would be the possibility to continuously upgrade the product post-sale without any type of physical movement (of either the product or a service technician).

Furthermore, some types of economic concepts that in themselves are "classic" have been dramatically changed. Marketplaces have been around for the past millennia but online marketplaces have virtually unlimited capacity of buyers and sellers without the need for geographical proximity. Payment between two economic actors of remote positions can be done in an instant. Firms can perform more accurate analyses of consumer preferences and behaviour based on enormous amounts of data within a short period of time. It is also possible to follow the operations of a machine in real-time, which can help to ensure its proper functioning and optimal energy usage, providing important insights on how to upgrade future versions or models of the product.

As such, data can be said to be an asset for firms – a type of semi-tangible asset, somewhere between tangible assets (such as capital and labour) and intangible assets (such as a strong brand or organisational culture). The Financial Times recently argued that "*Well-managed companies enjoy many advantages: strong brands, masses of consumer data, valuable historic data sets, networks of smart people and easy access to capital*".[5]

---

[4] OECD, 2013, "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value", *OECD Digital Economy Papers*, No. 220, OECD Publishing.

[5] Financial Times, February 1, 2016, "The path to enlightenment and profit starts inside the office" http://www.ft.com/intl/cms/s/0/d442ff7c-c67d-11e5-b3b1-7b2481276e45.html#axzz3yu2dL0yt

In today's globalised world, if something is important for businesses it means, almost per definition, that it is also important to be able to transfer it between countries. Data on e.g. customers, employees or research results are transferred, either in-house or at arms-length, within jurisdictions and across borders. In order to serve a foreign market, firms must be able to analyse what their customers want, advertise, provide smooth ordering, payment and delivery methods, provide post-sales activities and manage day-to-day operations. In other words, the same things every firm has to do to stay competitive.

If the ability to transfer data across borders is inhibited (or prohibited), foreign firms are put at a competitive disadvantage vis-à-vis domestic firms who do not face such barriers. Thus, trade is hindered, affecting not only the flows of digital products but all types of goods and services; the effects are felt by both end-customers as well as downstream producers.[6]

2.1 Data flows in the internal market

The internal market is of course no exception to the characteristics mentioned above. In fact, since the internal market is the most deeply integrated economic area among sovereign states, the relatively "new" issue of data flows is perhaps even more elevated than elsewhere in the world. Although far from being "complete" or "finished", the internal market has successfully removed several trade barriers, particularly for the trade in goods but also in services to some extent, as well as removing restrictions to the mobility of capital and persons. It has also provided an institutional framework for how to go about new barriers to those flows.

Therefore, the increasing importance of data for firms' competitiveness, coupled with the relatively low pertinence of barriers to the other flows in the internal market, makes for an interesting situation for the established framework to handle. Specifically, it is the increased collection, storing and processing of *personal* data that has attracted increased attention from the EU legislator.

The recently adopted Data Protection Regulation defines personal data as "*…any information relating to and identified or identifiable natural person…*"[7]. The National Board of Trade has previously[8] listed various types of personal data used by companies, divided into five distinct categories, all of which possibly containing personal data according to the definition in the Data Protection Regulation:

[6] Van der Marel et al., 2015, "A methodology to estimate the costs of data regulations", International Economics.
[7] Regulation (EU) 2016/679, Article 4.1.
[8] National Board of Trade, 2014:1, "No Transfer, No Trade – the Importance of Cross-Border Data Transfers for Companies Based in Sweden".

- **Corporate data** (such as data about the company, including financial data, aggregated numbers about employee and website).
- **End-customer data** (such as data about private persons, including name, address, bank account, credit reports, phone number, and localisation of the phone).
- **Human resources data** (such as data about employees, including names, e-mail addresses, salaries and competencies),
- **Merchant data** (such as data about other companies, including name, address, contact person, customer registry, website and financial transactions data).
- **Technical data** (such as data about products, services and technical solutions, including the operation of these).

2.2 Personal data in the internal market

The purpose of the internal market is to enhance the opportunities of economic prosperity in the EU through increased specialisation and trade. The free flows of the inputs and outputs of production (i.e. goods, services, capital and persons), coupled with establishment rights, means that citizens and firms can reap the benefits of a large, borderless market. Firms can reach more customers, and customers enjoy greater choice and lower prices. From this point of view, personal data must be able to flow freely within the internal market, since it too is an essential aspect of doing business and/or consumption today. This has already been acknowledged by the European Commission, given that one of the actions in the Digital Single Market Strategy is termed, among other things, the free flow of data.[9]

However, data is already very mobile. While the overarching objective of the original freedoms was/is to *increase* the respective flows, the issue of the free flow of data is rather centred on how to minimise negative externalities or other issues that may arise from transferring personal data between different jurisdictions. Data flows are global in nature and data is transferred around the around the world with technical ease. This makes it unchartered territory for the internal market regulatory framework, at least in relation to the existing freedoms.

Additionally, realising the original freedoms across the internal market meant that the various national goods, services, capital and labour markets were to be made one, larger, common market. The free flow of data is not about fusing the Swedish, German, Italian, Bulgarian etc. national data

[9] European Commission, 2015, "A Digital Single Market Strategy for Europe", COM(2015) 192 final, p. 20.

markets into one, since there are not really any national data markets. While data is certainly sold in some instances, one cannot usefully infer the value of personal data by looking at the market clearing price of data and/or by looking at the valuation of firms whose primary asset is personal data.[10]

The market-clearing mechanism, prevalent in the goods, services, capital and labour markets, does not readily exist for personal data. It does when it comes to *selling* personal data for e.g. advertising purposes (e.g. when Facebook sells ads), but it does not when data is transferred but not sold (e.g. when a firm collects *and* uses the data itself, which obviously carries great value for the firm but it is very difficult to estimate how valuable it is). Additionally, even when data is *sold*, it is not always clear-cut whether it is actually the data that is sold in itself or rather a service (which thus would fall under the free movement of services) that is built on data. Still, there is great value in data and the ability to transfer it between countries.

In an internal market context, the free flow of data should be understood in relation to how it affects the freedoms currently enshrined in the Treaty. Firms and consumers increasingly use cloud services, online platforms and marketplaces to do business in the internal market (including the so called collaborative economy). Many of those transactions are enabled through storage and processing of data on servers located outside the EU. Barriers to the transfer of data to third countries may therefore effectively constitute barriers to intra-EU movement of goods, services, capital and/or persons. This issue is discussed in more depth in Section 4 of this report.

2.3 Data flows around the world and privacy concerns

McKinsey Global Institute has in a recent report showed that the flows of data between regions of the world were 45 times larger in 2014 than they were in 2005.[11] While the global flows of goods, services and financial capital have come to a halt in recent years, data transfers seem to be the new driver of globalisation. However, the different types of flows are not separated from each other. The report by McKinsey has a useful example: "*Virtually every type of cross-border transaction now has a digital component. Container ships still move products to markets around the world, but now customers order them on digital platforms, track their movement using RFID codes, and pay for them via digital transactions*".[12]

[10] OECD, 2013, "Exploring the Economics of Personal Data: A Survey of Methodologies for Measuring Monetary Value", *OECD Digital Economy Papers*, No. 220, OECD Publishing.
[11] McKinsey Global Institute, 2016, "Digital Globalization: The New Era of Global Flows", Executive Summary. Data flows are measured as the usage of cross-border bandwidth between North America, Latin America, Asia, Europe, Middle East, Africa and Oceania. Intra-regional flows are not included.
[12] Ibid, p. 30.

Moreover, the development of 3D printing may further digitise the trade in goods, thus reducing the need for e.g. container ships.

A sizable share of the 2.5 quintillion bytes of data that is generated globally every day[13] is personal, in the sense that it can be traced back to an identified or identifiable natural person. Since much of this data is transferred around the world, governments and citizens have become increasingly wary about how this personal data is handled. In particular, discrepancies between how countries regulate the rights to privacy have become a more prominent problem, given the ease with which personal data can be accessed by a firm and/or public authority abroad. Countries with strict privacy regulations may for instance not be able to safeguard the rights of their citizens once their personal data is transferred to entities located in less protective jurisdictions. This in turn raises the desire for countries with strict privacy rules to export their regime abroad or at least limit the transfer of personal data to only be allowed to countries with adequate protection.

3 Identifying the restrictions to the free flow of data – A negative approach

As mentioned in the introduction, the EU legislator started to regulate the free flow of data as a reaction to the barriers that were erected by the Member States. The main concern was the fragmented regulatory framework for the protection of privacy and personal integrity. In addition, other types of barriers have come to play a role in defining the rules on movement of data, such as technical restrictions due to limited network capacity, security-related barriers and rules motivated by the protection of intellectual property rights.[14] We examine each of these barriers and their impact on the free flow of data in this section.[15]

[13] http://www.vcloudnews.com/every-day-big-data-statistics-2-5-quintillion-bytes-of-data-created-daily/. One quintillion = 10^{18}, i.e. 1 followed by 18 zeroes.

[14] Note that this is not an exhaustive list, other barriers may for instance relate to the protection of trade secrets, combating hate speech or protecting minors. See the Commission proposals for directives on the protection of undisclosed know-how and business information (COM (2013)813 final) and on the amendment of the Audiovisual Media Services Directive (COM (2016)287 final). A number of barriers may also relate to localisation requirements in respect of i.a. financial data (see National Board of Trade "Online Trade, Offline Rules" (2015), p. 32).

[15] Outside the EU, prorectionist measures also limit the free flow of data. Those measures described notably in the National Board of Trade's report "No Transfer, No Trade" (2012) do not however concern the internal market and are therefore not examined further in this report.

3.1 The protection of privacy and personal integrity

In the current European debate on the free flow of data, one of the main concerns is how this freedom impacts on the right to privacy and the protection of personal integrity.

Right to privacy

The right to privacy is a human right which protects certain aspects of an individual's life (body, property, identity, thoughts, feelings, personal relations, etc.) from being accessed by other individuals, organizations or the state.

There is not a single definition of the right to privacy. Rather its scope varies between countries and legal traditions. Its importance however is reflected in the fact that it is protected by most constitutions in the Western world and is enshrined in such fundamental texts as the 1948 Universal Declaration of Human Rights (Article 12) and the 1950 European Convention on Human Rights (Article 8).

The right to privacy is also safeguarded by the Charter of Fundamental Rights of the European Union (Articles 3, 7 and 8) which, after the entry into force of the Lisbon Treaty (2009), constitutes an integral part of the EU Treaties (so called "EU primary law").

3.1.1 How the free flow of data impacts on privacy

To the extent that data relates to identifiable individuals (so-called "personal data"), its transfer or processing may lead to sharing personal information with other persons or organizations.

Sharing personal information is not *per se* a problem and is indeed often volunteered by private persons, for example on social media or in e-commerce transactions. It may also have a positive impact on individuals, for instance in improving the use of personal devices connected to the internet (so-called "Internet of Things").[16] In many instances, the use of personal data aims at facilitating research and development as well as safeguarding a high quality level for the services offered to internet users. For example, part of the success of Netflix is its ability to process personal data (here past viewing experiences) in order to provide content adapted to each subscriber's preferences.

The sharing of personal data may however become an issue if the persons concerned feel that they lack control over which information is shared, with whom it is shared and for what purpose. This may be all the more problematic that the transfer and processing of data is a complex operation which involves many players (including intermediaries such as ISPs and cloud service providers) and a high level of digital competence to

[16] See National Board of Trade "No Transfer, No Production".

comprehend. An average person – internet user or not – is therefore unlikely to have full understanding over the use of its personal data.

This uncertainty is the main source of distrust among internet users.

In the worst case, personal data – they fear – may be used for fraudulent purposes (for instance phishing), or at least to their detriment. That would be the case of an insurer charging an insured person a higher premium on the basis of personal data showing poor health condition, or an employer questioning the suitability of an applicant in the light of that person's activities on social media.

In other cases, the sharing of personal data may simply constitute a nuisance for the individuals concerned. For instance, the use of a person's preferences, tastes or activities for the purpose of unsolicited marketing can for some be a source of irritation.

More generally, certain persons may be more sensitive than others to sharing personal information even if this does not automatically lead to concrete harm or disturbances. The level of tolerance towards such information sharing varies not only between individuals (and generations) but also between countries.[17]

3.1.2 Philosophical and ethical dimensions

Put in a bigger context, the sensitivity of individuals to information sharing is to be understood in light of the classical distinction between the private and public spheres of society. Introduced in Western philosophy by the ancient Greeks[18] and developed by legal scholars and thinkers in the last two centuries,[19] the separation between the two realms is an intrinsic component of Western societies.

The boundaries between the private and public spheres have shifted over time. Traditionally the private sphere referred to the family or home whereas the public sphere covered the remaining parts of one's life (for instance public activities). The emergence of the internet is challenging these boundaries and makes the traditional distinction between those two realms obsolete. Whereas most individuals' activities belonged to the private sphere since the industrial revolution, the reverse seems now to be true for many with the digital revolution. The introduction of new concepts

[17] This is reflected in the level of privacy regulation of each EU Member States. For instance, whereas the German Data Protection Act requires the appointment of a data protection officer for all companies with at least nine people employed in the automated processing of personal data, or at least 20 people who are engaged in non-automated data processing; the Swedish rules on data protection only provides for the appointment of a Personal Data Representative on a voluntary basis..

[18] See the Aristotelian distinction between *oikos* (home) and *polis* (city).

[19] See for instance J. Wagner DeCew "In Pursuit of Privacy: Law, Ethics and the Rise of Technology" (1997).

such as “citizen-consumer” and "market society”[20] reflects this paradigm shift.

Thus, the debate on privacy and data flow is not merely one of legal technicalities, missed business opportunities or of different anonymizing techniques but touches upon fundamental issues for individuals and the societies they live in. It is important for the legislators and all other interested parties to take into account these philosophical and ethical dimensions in order to address the potential conflicts between data flows and the right to privacy.

3.1.3 The role of the EU legislator

The pace of technological development is so fast that individuals do not always have the ability to grasp it and to adjust their own boundaries between what they consider as public and private information. This confusion at individuals’ level makes it difficult for the national legislators to adopt a consensual position. This is particularly problematic for the EU legislator which, in addition to managing the varying expectations of individuals and of businesses, must take into account the sensibilities of each Member State on privacy issues.

However, the issue for the EU legislator is not limited to weighing in all those interests in order to define an acceptable level of information sharing and processing. Given the complexity of data processing and management, the EU legislator also needs to ensure the control of such operations (i.e. avoiding any fraud or abuse) and that the rules are adapted to on-going and future technological development.

The EU legislator has taken a strong stance in balancing the right to privacy with the free flow of data with the adoption of the 1995 Data protection Directive and now the 2016 Data Protection Regulation.[21] Priority in EU law is granted to the right to privacy, which means that the flow of data is free only insofar as it does not restrict individuals’ privacy and personal integrity. In practice, this means that personal data may chiefly be processed and transferred if consent from the individuals in question has been granted.

---

[20] See for instance M. J. Sandel: “*This is a debate we didn’t have during the era of market triumphalism. As a result, without quite realizing it – without ever deciding to do so – we drifted from having a market economy to being a market society. The difference is this: A market economy is a tool – a valuable and effective tool – for organizing productive activity. A market society is a way of life in which market values seep into every aspect of human endeavor. It’s a place where social relations are made over in the image of the market. The great missing debate in contemporary politics is about the role and reach of markets. Do we want a market economy, or a market society? What role should markets play in public life and personal relations?*” (The Atlantic, “What Isn’t for Sale?”, April 2012).

[21] Directive 95/46/EC and Regulation 2016/679/EU.

The position of the EU legislator is motivated by a number of factors.

First, the right to privacy is deeply rooted in European traditions. As mentioned, it may vary between countries but those with the stricter rules, such as Germany and France, are not ready to compromise on this right. Europe's history, dominated with wars and totalitarian regimes, has created a strong aversion towards all-controlling entities. In respect of digital data, this aversion is fuelled by the sense of powerlessness some individuals may have in front of an unfathomable technology. As described above, the lack of understanding for how personal data may be used plays a heavy role in setting up adequate mechanisms for monitoring the way data is processed and transferred.

Second, and related to the first point, the tensions between the free flow of data and the right to privacy is not necessarily seen as a conflict between individuals and business interests. Several organizations, including the European Commission, have argued that strict privacy rules will foster trade.[22] Stricter rules, they argue, are necessary to enhance consumer trust and thereby removing one of the main barriers to e-commerce. Some businesses have also used their establishment in countries with strict privacy rules, or "Data Sanctuaries",[23] as a selling argument to attract sceptical customers.[24]

---

[22] See the Commission Communication supporting the proposal for a new Data Protection Regulation: "*The new rules will also give EU companies an advantage in global competition. Under the reformed regulatory framework, they will be able to assure their customers that valuable personal information will be treated with the necessary care and diligence. Trust in a coherent EU regulatory regime will be a key asset for service providers and an incentive for investors looking for optimal conditions when locating services.*" (Commission Communication "Safeguarding Privacy in a Connected World – A European Data Protection Framework for the 21st Century", COM (2012)9 final, p.8). Similar statements were made by the Commission, four years later: "*The data protection reform will help businesses regain consumers' trust to use their services. According to a 2015 Eurobarometer survey, eight out of 10 people feel that they do not have complete control of their personal data. Two-thirds of people are concerned they do not have complete control over their personal data online. Businesses that fail to adequately protect individuals' personal data risk losing their trust. This trust, particularly in the online environment, is essential to encourage people to use new products and services.*" ("Fact sheet EU Data Protection Reform – What benefits for businesses in Europe?" (January 2016)).

[23] Matthew Berger "Germany: Europe's Privacy White Knight?" (LinkedIn, March 22, 2016) (https://www.linkedin.com/pulse/germany-europes-privacy-white-knight-matthew-berger-cipp-us?trk=pulse-det-nav_art).

[24] This was for instance the case with Microsoft which motivated the opening of two data centers in Germany, one of the most protective countries in terms of privacy, by the need to reach out to customers with strong privacy concerns. See Wall Street Journal "Microsoft Offers EU Customers Option to Store Data in Germany" (November 12, 2015) (http://www.wsj.com/articles/microsoft-tightens-eu-clients-data-protection-1447247197). Similarly, Dropbox' recent move to Germany was viewed as a "*major selling point for Dropbox Business storage*" (see eWeek "Dropbox Expanding Into Europe, Will Host Customer Data in Germany" (February 11, 2016)

Third, the EU legislator is bound by a number of rules on privacy, not the least the Charter of Fundamental Rights of the European Union. The Charter, which constitutes an integral part of EU primary law, protects explicitly the right to privacy in respect of personal data.[25] Thus any secondary legislation adopted at EU level on the free flow of data has to comply with the level of protection of privacy set in these higher norms.

3.2 Technical barriers – No Network, No Transfer

It is an obvious truth that data cannot move on its own but needs support from a computer network, be it cable or wireless. Travelers abroad know all too well that, in the absence of WiFi (and unless they are ready to pay roaming charges), they will not be able to transmit any data. However, the mere existence of a network connecting the sender and the receiver of data is not a sufficient guarantee for a smooth data flow. Network capacity may for instance be limited and lead to congestion problems if the volume of data transmitted is too big.[26]

3.2.1 Network capacity limitation

Neither cables nor the radio spectrum have unlimited capacity to transfer data at the speed and robustness many of the digital services require. For example, the European Commission has communicated that regional authorities across the EU should reallocate the frequency band currently used for TV services in order to make room for the development of 5G mobile technology.[27] 5G, being approximately 100 times faster than 4G, is necessary to sustain self-driving cars, for example.

A report for the Swedish Ministry of Enterprise and Innovation stated that the increasing demand for mobile capacity cannot be met through extending mobile networks into new frequency bands – frequencies are a finite resource and they are nearly fully utilized.[28] Instead, a higher concentration of base stations is needed. However, they are a costly investment, and it is by no means certain that the investing operator will be

(http://www.eweek.com/storage/dropbox-expanding-will-build-new-data-center-in-germany.html).

[25] Article 8 (Protection of personal data) of the Charter reads: "*1. Everyone has the right to the protection of personal data concerning him or her. 2. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified. 3. Compliance with these rules shall be subject to control by an independent authority.*"

[26] This section focuses on technical barriers within the EU. There are, however, a range of technical barriers at the global level, see World Economic Forum, 2016, "Internet Fragmentation: An Overview", for a useful review.

[27] Financial Times, February 22, 2016, "Europe and Asia in race to set 5G mobile standard".

[28] A-focus, 2015, "Digitala tjänster: Gemensamma regler ger tillväxt i Europa".

able to profit from the investment through the increased demand it enables. The report's recommendation is therefore to allow for rival operators to jointly invest in base stations, since it has not been shown that it affects their competition for end-consumers.

Furthermore, various experts state that the EU is lagging behind the US in terms of (fast) broadband deployment.[29] It is argued that the American way of regulating the market has been more successful in promoting investment in modern broadband technologies, while the European regulation has rather encouraged operators to compete on existing networks. The European Parliament has called for a regulatory environment that encourages market actors to undertake necessary investments in broadband infrastructure.[30] Furthermore, there are substantial differences in coverage of so-called Next Generation Access networks (i.e. fibre-based high-speed networks) across EU member states.[31] The issue of network capacity also plays into the privacy aspect of data transfers, since high-quality networks are necessary to utilize more advanced security measures.[32]

3.2.2 Net neutrality as a guiding principle

A prominent issue regarding the technical capacity to transfer data is that of net neutrality. Essentially, it means that no data packages (i.e. a data "signal") should be given priority over other data packages. As such, "queues" are formed when there is too much data traffic in the network, and the users experience slower and/or lower quality connections. However, it is technically possible to prioritize some data packages over others, but the question is if it should be allowed or not.

At first glance, it may seem democratic to establish net neutrality, where no prioritization is allowed. Incumbent service providers would not be able to stifle competition through striking a deal with an operator to give their data priority over their rivals. However, some types of digital services are more sensitive to the connection speed and quality than others. For example, sending an e-mail is not very sensitive, while a video call is (and even more so, self-driving cars). Therefore, it may be beneficial if some data packages could be prioritized over others. The challenge for the regulator is to establish rules that enable prioritization for sensitive services over insensitive ones, while at the same time maintaining neutrality among

[29] Yoo, Christopher S., 2014, "U.S. vs. European Broadband Deployment: What Do the Data Say?", University of Pennsylvania Law School, Center for Technology, Innovation and Competition.
[30] European Parliamentary Research Service, 2015, "Broadband infrastructure – Supporting the digital economy in the European Union".
[31] Briglauer, W., Cambini, C., and Grajek, M., 2015, "Why is Europe Lagging on Next Generation Access Networks?", Bruegel Policy Contribution.
[32] National Board of Trade, 2015, "No Transfer, No Production", Kommerskollegium 2015:4.

providers of the same type of service (i.e. to not allow priority for one provider of video calls over another).

The EU legislator has taken a stance on this issue with the adoption of the Regulation on Open Access Internet which entered into force in April 2016.[33] The Regulation provides for net neutrality and forbids the Internet Service Providers from blocking, throttling or discriminating internet traffic except in specific situations.[34] In that respect, the EU is in line with the US position which had already endorsed the principle of net neutrality.[35] This position is however subject to challenge before the US courts and several ICT companies have argued that net neutrality would have a deterrent effect on future investment in network infrastructure.[36]

3.3 Security-related barriers

Crime knows no borders and that is all the more true in respect of terrorism. Recent terror attacks have highlighted the need for countries to collaborate with each other and exchange information related to potential threats. More generally, police and judicial cooperation across borders in criminal matters is an essential part of the Area of Freedom, Security and Justice, itself a pillar of the EU. The free flow of data is a prerequisite for such cooperation.[37] It would therefore seem natural to see national security interests and the free flow of data going hand in hand, at least in the EU.[38]

However, the last years have seen growing tensions between certain national security interests and privacy rights. As a result, a number of national security measures aiming at facilitating the free flow of data have been blocked or delayed in the EU. That is the case of the Data Retention Directive[39] which was found to breach the privacy rights of individuals and

[33] Regulation 2015/2120/EU.
[34] Those are compliance with legal obligations, integrity of the network and congestion management in exceptional and temporary situations (Article 3(3) of the Regulation).
[35] Federal Communications Commission (FCC) "Protecting and Promoting the Open Internet" (2015) (https://www.federalregister.gov/articles/2015/04/13/2015-07841/protecting-and-promoting-the-open-internet).
[36] See for instance the letter of opponents to the net neutrality principle addressed to members of the US Congress and FCC (10 December 2014) (http://www.tiaonline.org/sites/default/files/pages/Internet_ecosystem_letter_FINAL_12.10.14.pdf).
[37] In general, the free flow of data between the different public bodies of the EU Member States is an important tool in ensuring the functioning of the internal market. Instruments such as IMI do encourage the exchange of information between national authorities, and in some cases make it compulsory to share such information across borders.
[38] Save for the blocking of illegal information (such as child pornography, terrorist and other criminal activities) which in principle can be construed as a restriction on the free flow of data. This type of censorship falls however outside the scope of this report.
[39] Directive 2006/24/EC which aimed at the collection of personal data for the purpose of fighting crimes.

was therefore invalidated by the Court of Justice of the European Union (CJEU).[40]

Similarly, discussions on the sharing of personal data of passengers (so-called "PNR" or Passenger Name Records) between the US and EU have stalled for many years. After being quashed by the CJEU in 2006,[41] a new agreement on handovers of EU passenger information was finally approved by the European Parliament in 2012.[42] Critics of this and similar agreements with other third countries[43] have however been ongoing since then.[44] And it is only recently that, almost three years after a negative vote by the European Parliament, the EU legislator finally agreed on a Directive on the sharing of passenger information between the EU Member States.[45]

To some extent, the invalidation of the Commission Safe Harbour Decision by the CJEU in 2015 also illustrates the tensions between national security interests and privacy rules.[46] The Snowden revelations on the activities of the US National Security Agency triggered a complaint by a private person arguing that the transfer of his personal data to Facebook's servers located in the US was in breach of the EU rules on privacy. The CJEU noted in that respect that the Safe Harbour Agreement to which Facebook had subscribed did not protect the rights on privacy in an adequate manner. It stated notably that:

> "[the Commission Decision on Safe Harbour] *lays down that 'national security, public interest, or law enforcement requirements' have primacy over the safe harbour principles, primacy pursuant to which self-certified United States organisations receiving personal data from the European Union are bound to disregard those principles without limitation where they conflict with those requirements and therefore prove incompatible with them.*" (para. 86)

The prevalence of national security interests by the US authorities over the right to privacy enshrined in EU law, without effective legal protection

---

[40] Cases C-293/12 *Digital Rights Ireland* and 594/12 *Seitlinger and Others*.
[41] Joined Cases C-317/04 and C-318/04 *European Parliament v. European Council and Commission*.
[42] Agreement between the USA and the EU on the use and transfer of passenger name records to the US Department of Homeland Security (OJ L 215, 11.8.2012).
[43] The agreement between the EU and Canada was recently deemed "clearly incompatible with the EU Charter" by Advocate General Mengozzi - Opinion 1/15 8 September 2016
[44] See letter dated 6 January 2012 of the Article 29 Working Party (grouping the national data protection authorities of the EU) on the draft PNR Agreement with the USA. Note also that a case is currently pending before the CJEU on the compatibility of the EU-Canada Agreement on PNR with privacy rights (case A-1/15).
[45] See press release 176/16 from the European Council "Council adopts EU Passenger Name Record (PNR) directive" (21 April 2016).
[46] Case C-362/14 *Schrems*.

against such interference, was found by the CJEU to constitute grounds for invalidating the Commission Safe Harbour Decision.

Clearly, the cases mentioned above show how the free flow of data becomes a collateral victim of the tensions taking place between the right to privacy and national security interests. In that respect, the repeated stances of the CJEU make it plain that the protection of the right to privacy has priority over the free flow of data, even when the latter is justified by the fight against crime.

3.4 The protection of intellectual property rights

The territorial nature of intellectual property rights may lead to restrictions to the free flow of data. To the extent that data relates to protected works – for instance a movie, music, a software or an e-book – it may only be used within the territory for which a license has been granted. Such data may therefore not be transferred freely outside the licensed territory.[47]

The issue becomes especially problematic in the case of digital content which is made available to consumers in those territories for which a license has been obtained but are stored in the cloud located in non-licensed territories. In the case of movies for instance, the absence of a license covering the place where data is stored may lead to copyright infringements.

These issues may be solved in different manners, for instance by way of contracts or relying on certain legal exemptions.[48] Ultimately however, the risk of copyright infringement may require blocking data from being accessed in non-licensed territories (so-called geo-blocking). The EU legislator is currently considering the adoption of rules limiting geo-blocking but those should not affect situations where the blocking of data is motivated by the protection of intellectual property rights.[49]

3.5 Conclusions

Although the free flow of data is sometimes taken for granted, the many restrictions examined here show the need for rules that remove or at least mitigate hinders to that flow. As shown in this section, the EU legislator has adopted a number of measures in respect of data movement. Proponents of the freedom of movement of data may however have some concerns with regards to these measures:

---

[47] See ”Online Trade, Offline Rules” (National Board of Trade, 2015).
[48] Such exemptions are for example set under the E-Commerce Directive (2000/31/EC) in the case of hosting services (Article 14) and the Directive on Information Services (2001/29/EC) in the case of reproduction rights (Article 5).
[49] Commission Communication ”A Digital Strategy for Europe” (COM (2015)192 final).

- The Data Protection Regulation gives priority to the protection of personal data over data flow;
- The EU rules on net neutrality may have a deterrent impact on the development of broadband capacity, itself a key factor for data flow;
- The EU is lacking rules that would mitigate IP-related restrictions on the free flow of data.

Given the above, we examine in the next section how the EU rules on data compare to the classic freedoms of goods, services, persons and capital that constitute the backbone of the internal market.

4 Relations to the four freedoms – A comparative approach

Data does not qualify as goods, services, persons or capital. This is not to say that the free flow of data automatically falls outside the scope of the four freedoms. Rather, in the absence of harmonisation measures, restrictions on the free flow of data may be tested against different Treaty freedoms depending on the nature of the transaction at stake. Hence, a restriction on the processing of data that would fall outside the scope of the Data Protection Directive – for instance a restriction on non-personal data (e.g. financial or accounting data) – may be assessed in the light of the Treaty rules on services (Article 56 TFEU) when it affects the activities of a service provider or of the Treaty provisions on capital (Article 63 TFEU) when it hinders the free movement of capital.

However, most of the restrictions on the flow of data would be covered by secondary legislation, notably the Data Protection Directive and, as from 2018, the Data Protection Regulation. These measures provide for a set of rules that is distinct from the other four freedoms. Interestingly in that respect is that whereas the 1995 Data Protection Directive uses the internal market harmonisation provision (Article 114 TFEU) as a legal basis, the 2016 Data Protection Regulation instead refers to the Treaty rules on the protection of privacy (Article 16 TFEU).

Thus, the rules on the free flow of data are distinct from those on the four freedoms, either because they fall under an own set of rules or because they are covered by several of the four freedoms, rather than by any specific one.[50]

In this section, we examine briefly the similarities between the free flow of data and the four freedoms (**Section 4.1**) and highlight the main differences between these sets of rules. The two main ones concern, in our view, the position of the EU rules on data movement in the EU regulatory framework

[50] Note in that respect the discrepancies between the four freedoms discussed in "Freedoms Without Borders" (National Board of Trade, 2015).

(**Section 4.2**) and the uncertainty surrounding the very concept of the free flow of data (**Section 4.3**).

4.1 Similarities with the four freedoms

The similarities between the free flow of data and the traditional freedoms of movement of goods, services, persons and capital are obvious. Indeed, all aim at the functioning of the internal market. In the same way as capital or labour (persons), data has become a valuable input for companies and its free flow is necessary for businesses to perform.

Both the rules on the free flow of data and on the traditional freedoms aim at balancing pro-integration arguments with the protection of legitimate national interests. They all target national barriers (protectionist or incidental) and call for their removal.

They also provide for a common regulatory framework at the EU level, harmonize national legislations and set up coordination mechanisms (such as the WP29[51]) in order to avoid divergent administrative practices within the Union. To the extent that a barrier on the free flow of data is falling outside the scope of harmonization measures, the same principles of non-discrimination, mutual recognition and proportionality would apply as for the traditional freedoms. Yet, as seen below, a number of significant divergences remain.

4.2 An ancillary freedom

There are two sets of rules in the EU: those defined in the EU Treaties (primary law) and those set out in EU legislation such as regulations, directives or Commission decisions (secondary law). Whereas primary law gives the main direction of EU integration, secondary legislation implements the principles set in the EU Treaties. In the hierarchy of norms, primary law is superior to secondary legislation. In practice, this means that a piece of secondary legislation may be invalidated if it conflicts with principles set in the EU Treaties.

The four freedoms are an integral part of primary law. They are introduced in the EU Treaties and constitute the pillars upon which the internal market is built. Numerous rules of secondary law have been adopted by the EU legislator in order to facilitate the free movement of goods, services, capital and persons but all of them rely on the principles of non-discrimination,

[51] The Article 29 Working Party (WP29) groups together representatives of the national and EU Data Protection Authorities as well as the European Commission. It aims at coordinating national data protection policies and to maintain a uniform interpretation of the EU rules on data protection. As from 2018, the WP29 will be replaced by a European Data Protection Board in accordance with the new Data Protection Regulation.

mutual recognition and proportionality defined in the EU Treaties for each freedom.

The free flow of data on the other hand is not explicitly set in the EU Treaties. Unlike the traditional freedoms, it is introduced, defined and regulated through acts of secondary law such as the Data Protection Directive (1995) and the newly adopted Data Protection Regulation (2016). Legally speaking, the free flow of data is subordinated to the other freedoms and other primary rules.

Not only do the rules on data rank lower than those on the traditional freedoms, but the very interest which potentially clashes with the free flow of data – the right to privacy – is itself enshrined in the EU Treaties. As mentioned above,[52] the right to privacy is safeguarded by the Charter of Fundamental Rights of the European Union which, since the Lisbon Treaty, forms an integral part of EU's primary law. It is also protected under an own provision of the Treaty.[53] This explains why pieces of secondary legislation on data, such as the Data Retention Directive or the Commission Decision on Safe Harbour may be invalidated for breaching the primary rules on the right to privacy.

The difference of status between the traditional freedoms and the free flow of data is not purely legalistic. It also reflects the ancillary role granted by the EU legislator to the movement of data in the functioning of the internal market. The texts of the main EU rules on data are in that respect revealing. Both the 1995 Directive and the 2016 Regulation concern the "*protection of individuals with regard to the processing of personal data and on the free movement of such data*".[54] However in practice, these acts mostly focus on the protection of individuals rather than the free movement of data. Even more so, whereas the 1995 Directive explicitly referred to the positive role of the free flow of data for trade, the 2016 Regulation only pays lip service to its importance.[55] In that respect, the absence of reference to the internal market harmonization provisions as a legal basis for the Regulation[56] shows that the connection between the EU rules on data and the functioning of the internal market is becoming weaker.

---

[52] See Section 3.1.3.
[53] Article 16(1) TFEU reads: "*Everyone has the right to the protection of personal data concerning them.*"
[54] The titles of these two acts are identical save for the wording "individuals" which in the 2016 version is replaced by "natural persons".
[55] Compare the preamble of the 1995 Directive, quoted in footnote 1 with the preamble of the 2016 Regulation which, out of 173 recitals barely acknowledges that "[t]*he proper functioning of the internal market requires that the free movement of personal data within the Union is not restricted or prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data.*" (Recital 13).
[56] As mentioned above in introduction to Section 4.

In other words, the newest rules on data flow are not so much concerned with the free movement of data as a means to foster the functioning of the internal market, but as a means to implement the primary rules on the protection of privacy. Thus, as opposed to the other freedoms and far from being considered as a driving force for European integration, the free flow of data seems to be viewed by the EU legislator as an impediment to the realization of some of the Treaties' objectives.[57]

4.3 An immature freedom

The freedoms of goods, services, persons and capital were introduced in the original Treaty of Rome in 1957. Save for the free movement of citizens which appeared first with the Maastricht Treaty (1992), the current freedoms have therefore been a part of the internal market for almost 60 years. During this long period of time, the rules have been interpreted by the CJEU and detailed by the EU legislator to a degree that the principles on which they rely remain stable and predictable.

There may of course be surprises, such as when the CJEU introduced the principle of mutual recognition[58] or reverted its case law on the concept of quantitative restrictions.[59] The increasing workload of the CJEU also shows that numerous uncertainties remain as to the application of the four freedoms in concrete situations. This is especially true in respect of new EU Member States or with the emergence of new technologies and markets. Overall, however, there is a general understanding among all parties concerned (notably the EU Member States, businesses and private persons) on the content of the four freedoms.[60]

In our view, the freedom of data has not reached that degree of maturity. After twenty or so years of existence, the rules on data flows have not yet gone into an administrative phase. Instead, the EU legislator and national regulators are still struggling with fundamental issues, the main one being the balancing of the free flow of data with the right to privacy.[61] In that respect, the recent rulings of the CJEU on data protection[62] are

---

[57] Here an "*area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.*" (Recital 3 of the 2016 Data Protection Regulation).
[58] Case 120/78 *Cassis de Dijon*.
[59] Joined cases C-267/91 and C-268/91 *Keck and Mithouard*.
[60] This is not say that all restrictions have been removed but rather that the findings of such restrictions seldom come as a surprise.
[61] Although too early to assess, the strong stance in favour of the protection of privacy in the newly adopted Data Protection Regulation does not seem to bring a satisfactory answer to the concerns raised by businesses and other proponents of the free flow of data. See below Section 5 for the reactions of the ICT industry to the adoption of the Regulation.
[62] See notably case C-362/14 *Schrems* on the legality of the Safe Harbour Principles, case C-131/12 *Google Spain* on the so-called "right to be forgotten" and joined cases C-

symptomatic of the confusion surrounding the scope of the rules on the free flow of data.

This confusion may be explained by at least two main factors.

First, the significance of data processing is yet difficult to grasp.[63] The increasing dependency of modern economies on data present large possibilities in terms of productivity and efficiency but also potential drawbacks with regards to the integrity of individuals. Both those benefits and risks are hard to map out. This is all the more complicated since technologies are advancing more rapidly than the legislative process.[64] As a result, there is a lack of consensus on what would constitute an acceptable level of risk exposure and correspondingly an acceptable level of restriction on the free flow of data.

Second, the freedom of movement of data makes sense if it is global rather than regional. Unlike goods, services and persons, data may not easily be confined to a limited area, be it as vast as the EU. There are very few, if any, technical hinders to transferring data instantaneously across national borders and continents.[65] Intra-EU transactions would for instance typically require the transfer of data to cloud servers located somewhere outside the EU. Ensuring free movement within the Union will therefore only have limited significance if transfers to third countries are restricted or even prohibited. Confining the free movement of data to the territory of the EU, as is the case with current and incoming EU legislation, raises not only technical and commercial issues but also supervisory ones.[66]

As a result of these factors, the EU rules on data may not always be up-to-date, adequate or even applicable.[67] They contrast in that respect with the degree of maturity of the rules on goods, services, persons and capital.

293/12 and C-594/12 *Digital Rights Ireland* on the invalidation of the Data Retention Directive (2006/24/EC).

[63] Tillväxtanalys (2014), "Digitaliseringens bidrag till tillväxt och konkurrenskraft i Sverige", Rapport 2014:13. The report concludes that it is yet only the ICT sector that has managed to significantly increase its productivity through digitisation, but we have yet to see "across-the-board" productivity increases.

[64] See National Board of Trade "Online Trade, Offline Rules" (2015), Section 5.2.

[65] It may in that respect be more appropriate to compare data with capital rather than with goods, services or persons. Note however that whereas, as a matter of principle, EU law explicitly provides for the free movement of capital within the EU and with third countries, it does explicitly forbid the transfer of data to third countries.

[66] Technical and commercial issues include the designing of network infrastructures (routers, servers, etc.) complying with the EU prohibition on transfer of data to third countries whereas supervisory issues concern the setting up of control mechanisms that would effectively prevent the circumvention of this prohibition.

[67] See National Board of Trade "Online Trade, Offline Rules" (2015), Section 5.2.

4.4 Conclusions

There is no doubt that the free flow of data constitutes a freedom of movement in its own right under EU law. However, as shown in this section, this freedom is subsidiary to the Treaty rules and notably to the traditional freedoms of goods, services, persons and capital as well as to the interest it primarily conflicts with, the right to privacy. It has an ancillary function and lacks the level of maturity of the traditional freedoms of movement. This in turn affects the foreseeability and the visibility of the rules on data flows, of which the repeated invalidation judgments by the CJEU are symptomatic.

There is in our view a gap between the contribution of data flows to the functioning of the internal market and the way this freedom is promoted in internal market legislation. In the next and final section, we discuss this gap and notably the opportunity of strengthening this freedom at EU level.

5 Upgrading the freedom of movement of data?

The free movement of data can be assimilated to a natural right in the sense that it is pre-existent to the law rather than being made dependent on it. Businesses and internet users would assume that data moves freely over the borders not because the law permits it but because technology makes it possible. In fact the law, as we have seen earlier, has had the effect of restricting the free flow of data, be it in order to secure privacy rights or other legitimate interests.

These legal and judicial developments have been the root of calls for an upgrading of data transfers to a fifth freedom given the importance data has in our digital economy (5.1) Such appeals might be met both with legal arguments concerning the primacy of human rights within EU-law (5.2) as well as more political arguments regarding the relationship between privacy and data flows. (5.3) Our proposal is a new kind of proportionality assessment that takes both sides of the coin into perspective (5.4).

5.1 The importance of free movement of data

For a long time, there has been a tendency to take the free movement of data for granted, i.e. not necessarily worth protecting, at least not as much as the interests it conflicts with. Although attitudes may be shifting, this view seems to be prevalent with the EU legislator. Witness to that is the little attention paid to the free flow of data as such in the EU rules on data.[68]

[68] See above Section 4.2.

In the EU however, this view is questioned by some stakeholders.[69] The point of conflict focuses on the general prohibition to transfer personal data outside Europe which, as mentioned above, may also concern intra-EU transactions. Confirmed by the CJEU[70] and strengthened in the newly adopted Data Protection Regulation, the prohibition on transfer of data is not absolute but challenges a fundamental development of our digital economy: the storing of data in cloud servers located anywhere on the globe.

Some would predict catastrophic consequences for our economy with a too strict prohibition on data flow.[71] In that context, it is legitimate to discuss the appropriateness of upgrading the free movement of data as a "fifth" freedom on par with the traditional freedoms of goods, services, persons and capital. Such calls are not merely slogans, although their content is imprecise, but rather reactions to what is perceived as a real threat on an essential factor for the development of our modern economies.

In our view however, the introduction of a fifth freedom in the internal market architecture would merely have a symbolic value and not necessarily alter the current balance of interests between notably data flows and the protection of privacy.

5.2 The legal relationship between the right to privacy and data flows

First, it is unclear how the labelling of the free flow of data as a fifth freedom would translate in concrete terms. To gain parity with the four freedoms would require an amendment of the EU Treaties which in short to medium term may not be realistic. Another, less ambitious way to promote the freedom of movement of data would be for the EU to initiate measures to that effect. We note in that respect that the European Commission recently announced its intention to present a "European free flow of data

---

[69] See for instance the negative reactions of ICT businesses and stakeholders following the adoption of the 2016 Data Protection Regulation (GDPR): "*The Industry Coalition for Data Protection, an umbrella group that includes DigitalEurope, the World Federation of Advertisers, the Software Alliance and a number of others, described the GDPR text as "a wrong turn," with FEDMA Secretary General Sébastien Houzé declaring, "We are very concerned that investors will be scared off from investing in Europe and will build the next big thing in technology elsewhere, like Asia."*" (S. Pfeifle "GDPR: We Have Agreement" Privacy Tracker, December 16, 2015) (https://iapp.org/news/a/gdpr-we-have-agreement/).

[70] Case C-362/14 *Schrems*.

[71] See the reactions of some stakeholders and experts from the ICT industry following the invalidation of the Safe Harbour Agreement by the CJEU and the WP29 negative opinion on the new EU-US Privacy Shield Agreement (for instance https://www.theparliamentmagazine.eu/articles/eu-monitoring/eu-parliament-debates-eu-us-umbrella-agreement-personal-data, http://www.taylorvinters.com/news_and_events/article/safe-harbour-and-the-ecj-decision-on-the-schrems-case-697 or http://in.reuters.com/article/eu-privacy-facebook-idINKCN0YG2HD).

initiative".[72] It is at this stage too early to assess the content of such initiative. One may however expect an acknowledgement of the role of the free flow of data in the functioning of the internal market and the process of economic integration.

Second, it remains that the protection of privacy and personal integrity will always constitute a fundamental right enshrined in the EU Treaties. Thus, regardless of the form an upgrade of the free flow of data would take, this freedom would still have to comply with the basic requirements that today justify restrictions on the free flow of data.

5.3 Extenuating circumstances

In order to make a correct assessment of the problems caused by hampered data flows we also have to question the very nature and intensity of the conflict between the free flow of data and the protection of legitimate interests such as the right to privacy. We have already mentioned some arguments that have been put forth to nuance this opposition, notably that trade may benefit from stricter rules on data protection.[73] These arguments needs to be taken into account since the level of threat posed by strict EU privacy rules on data flows is dependent on market and regulatory developments.[74]

When stricter privacy rules are advocated, the argumentation may contain additional elements, such as: (i) the export of the stricter privacy regime put in place in the EU to other parts of the globe and (ii) the development of technological and commercial solutions that may mitigate the negative impact of privacy restrictions on data flows.

(i) The area with adequate protection might grow

Compared with other jurisdictions, notably the US, the EU has adopted a strict privacy regime. However, the EU does not stand alone, and it seems that a growing number of countries are considering similar regimes.[75] In terms of data flows, this is an important aspect since the greater coverage these rules will have,

---

[72] See the Commission's webpage on the Digital Single Market where the Commission states that "*the aim* [of the European free flow of data initiative] *is to promote free movement of data in the European Union. The initiative will tackle restrictions to data location and access to encourage innovation.*" (https://ec.europa.eu/digital-single-market/en/economy-society-digital-single-market).

[73] See Section 3.1.3.

[74] As would be the case in our proposal for a proportionality assessment below in section 5.3

[75] Aside from those countries mentioned below (footnote 72), Brazil is moving closer to the EU data protection regime and a number of Asian countries have recently adopted "European-style privacy rules", notably, Singapore, Japan, Malaysia and South Korea (see Hogan Lovells: "2015: The Turning Point for Data Privacy Regulation in Asia?" (http://www.hldataprotection.com/2015/02/articles/international-eu-privacy/2015-the-turning-point-for-data-privacy-regulation-in-asia/).

the less restrictions will occur on the free flow of data.[76] Thus it cannot be excluded that third countries find it necessary to adopt stricter privacy rules, if not out of concern for the privacy of their citizens, at least in order to gain access to the European market.[77] Note that the export of the EU regime also impacts intra-EU trade since it is common for transactions between entities in two EU countries to include the transfer of personal data outside the EU.[78]

It is however unlikely that the US will adjust its regime to the European one. Given the place of the US in the digital economy with most major ICTs being established on that side of the Atlantic, the EU prohibition on the transfer of data to third countries may have serious consequences. As mentioned, the Safe Harbour regime which constituted an exception to this prohibition was invalidated by the CJEU. A new regime, the EU-US Privacy Shield,[79] is being put in place but its validity is also questioned.[80] Regardless of these institutional discussions, one can see that technological and commercial solutions may enable firms to circumvent the gap between the two regimes.

(ii) Technological and commercial solutions might alleviate barriers to data flows

One possible way to legally circumvent the prohibition on the transfer of personal data to third countries is to "anonymize" or "de-identify" the data. However, it is still subject to an ongoing debate over its usefulness as a guarantor of personal privacy as it is argued that "de-identified" data can be "re-identified" without too much complexity.[81] [82]

---

[76] Under the Data Protection Directive (Article 25), the prohibition to transfer personal data outside the EU does not apply in respect of countries that have an "*adequate level of protection*". So far, the following countries have been found by the European Commission to provide such protection: Andorra, Argentina, Canada (commercial organisations), Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay (http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm).

[77] For a parallel, see the study "From Competition to Convergence – TTIP and the Evolution of Global Standards" (National Board of Trade, 2015) which shows how, in the field of standardization policy, the stricter European regulatory model was exported to third countries to the detriment of the US model.

[78] See above, Section 4.3.

[79] See the Commission press release "EU Commission and United States agree on new framework for transatlantic data flows: EU-US Privacy Shield" (2 February, 2016).

[80] See Opinion 01/2016 on the EU – U.S. Privacy Shield draft adequacy decision of the WP29 (13 April 2016).

[81] Cavoukian and Castro, 2014, "Big Data and Innovation, Setting the Record Straight: De-Identification *Does* Work", Information and Privacy Commissioner, Ontario, Canada.

[82] Narayanan and Felten, "No silver bullet: De-identification still doesn't work", Princeton University.

In order to counter the negative effects of the invalidation of the Safe Harbour regime, a number of ICT companies from the US have further relocated their servers to Europe.[83] In fact, new technological solutions and business models are being devised to secure the storage of personal data on European soil without interference from third country authorities.[84] Whereas a few years ago, it was maybe not so relevant to trace the exact movement of specific data, it becomes more desirable and feasible to reroute that data to a specific storage location with the EU ban on transfer to third countries.

This would suggest that the digital economy is not a passive victim of strict privacy rules, but instead rather capable of finding solutions that accommodate the concerns of the EU legislator.

5.4 Conclusions – the need for a new kind of proportionality

A call to upgrade the free movement of data to a fifth freedom should be seen in this light. Even if vigilance is necessary in order to avoid unnecessarily heavy and costly requirements on the flow of data, it is in our view unlikely that such an upgrading would significantly increase the protection of this freedom. Rather, a more realistic approach would be to consider the impact any new EU measures may have on the free flow of data given that: it is subsidiary to the protection of privacy (5.1) and such measures should be subject to a cost/opportunity assessment on businesses and technological development (5.2).

This approach is very similar to the proportionality principle applicable in respect of the four freedoms. It consists in acknowledging the primacy of legitimate interests and, without jeopardizing them, making sure that restrictive measures on the flow of data adopted at EU level do not go further than what is strictly necessary for the protection of these interests.

In that sense, this approach contrasts with the broad discretion enjoyed today by the EU legislator in adopting measures for the protection of privacy rights. Those measures may be quashed by the CJEU for being unnecessarily restrictive of privacy rights, as experienced in several recent cases, but most likely not for imposing an unnecessary burden on businesses and the free flow of data.[85]

---

[83] See the examples of Microsoft and Dropbox described above under Section 3.1.3.
[84] See for instance the third party models provided by Deutsche Telekom and by JotForm (J. Sanders "Cloud vendors seek refuge in Germany to comply with EU data laws" TechRepublic (November 13, 2015) (http://www.techrepublic.com/article/cloud-vendors-seek-refuge-in-germany-to-comply-with-eu-data-laws/)).
[85] This is all the more true in respect of the Data Protection Regulation that this measure only refers to the protection of privacy (Article 16 TFEU) as its legal basis. In other words, the objective of the Regulation, unlike that of the 1995 Data Protection

Note that such proportionality requirement is in theory already in place in accordance with Article 5 TEU. In practice however, it is questionable if such a test was properly conducted in relation to the burden imposed on businesses by the Data Protection Regulation. In particular, various experts have expressed concerns regarding the preparatory works of the Regulation[86] and its assessment of the costs potentially incurred by businesses in respect of the obligation to appoint a Data Protection Officer or of the right to be forgotten, suggesting that the costs may have been underestimated.[87] Nor do these documents discuss thoroughly the negative impact that such measures may have on innovation and the free flow of data.[88]

In the end, it might be so that such drastic obligations were the only means to achieve the high privacy standard set by the EU legislator. Our point with this example however is to illustrate the need of a thorough proportionality test focusing on the impact that EU measures may have not only on businesses (such as ICT companies) but also more generally on the free flow of data.

Directive, is not to strengthen the internal market as such (of which the free flow of data may be viewed as a component) but to secure a high level of protection of privacy.

[86] For instance, the Commission proposal itself (COM (2012)11 final), its accompanying Communication (COM(2012)9 final) and the Commission Impact Assessment (SEC (2012)72 final).

[87] Christensen and Etro (2013), "European data protection: Impact of the EU data-protection regulation" (http://voxeu.org/article/european-data-protection-impact-eu-data-protection-regulation).

[88] The Commission does discuss at length the positive impact that strict privacy rules may have on trade in terms of increased trust, but does not properly address concerns expressed by stakeholders in respect of a possible weakened innovation climate and competitiveness in the EU.