Athens Journal of Law - Volume 3, Issue 1 – Pages 21-30

International Trading of Big Data

By Davide Borelli[*]

The free movement of data is a prerequisite of the Digital Single Market and represents a conditio sine qua non for European companies' competitiveness which would suffer, in absence of it, a drastic downsizing. Nevertheless, personal data transfer would face considerable boundaries if a third country or an international organisation was involved.

Keywords: *data protection directive, general data protection regulation, data trading, cross-border data transfer and big data.*

Introduction

Every international transaction entails a data flow across national borders. We witness continuous information flows within business groups between subsidiaries established in different countries. The business network feeds on communications between partners, often scattered all over the world. In almost every situation, the information exchanged is able to identify an individual; for this reason, this information could be identified as personal data.

However, misuse of personal data is likely to harm fundamental values of human existence. Therefore, to ensure the economic, social and cultural development, it must be ensured that economic needs do not oppress human rights and fundamental freedoms. The balance between these disparate elements is managed – in most cases – under national sectoral legislation, as well as international treaties. In such a case, even the judgments of national courts play a crucial role in terms of interpretation and application of the rules on data protection: the balance *verbo tenus* needs, consequently, to be applied to each specific case, with more and different shades, which are not easily foreseeable ex ante.

Upstream of the balance mentioned above, the interests involved should be precisely identified: on the one hand the data controller's interests (which can be private or public), on the other hand those which refer to the individual concerned. In this regard, for example, does the protection of personal data, which is considered as a fundamental right, exclude a priori an individual's economic interest to which these data relate to?

The enforcement of the rules on data protection, as well as the determination of the judicial authority possibly responsible, is inextricably linked to the place where data are processed. If data are processed in a specific country, no doubt as to the applicable law may be raised. The situation,

[*] PhD Scholar in Law, Suor Orsola Benincasa University of Naples, Naples, Italy; Visiting PhD Scholar, the Institute of Advanced Legal Studies, University of London, UK.

https://doi.org/10.30958/ajl.3-1-2 doi=10.30958/ajl.3-1-2

however, becomes more complex if the processing involves more countries, realising, in this case, a cross-border data transfer.

Also in this case, therefore before to proceed with the evaluations on the potentially applicable law, it must be questioned what constitutes a cross-border transfer of data.

The Cross-border Data Transfer Phenomenon

The fundamental change in the way of processing personal data is due to the recent developments in the economic and technological environment: an example for this situation can be the implementation's effects of cloud storage systems and the Internet of Things (IoT).

In the last few decades, global economic integration pace is increased in intensity as a result of: (i) the recent developments in different fields (ranging from technology to logistics), and (ii) the liberalisation of international trades.

The latter took place, at first, through the signing of the GATT[1] and later thanks to the foundation of the WTO[2]. It cannot therefore be denied that the rise of globalization has played a key role in the transformation of the data processing operations[3].

Secondly, it must be considered the increasing economic importance of data processing: experts predict that revenue from the sales of big data, business analytics applications, tools, and services will increase more than 50% (from nearly 122 billion dollars in 2015 to more than 187 billion dollars in 2019[4]).

A further change in data processing operations is due to the current ubiquity of data transfers over Internet. If in the past a cross border data only occurred if there was a specific intent to internationally transfer data, nowadays the internet architecture itself implies that a transfer between two entities within the same country may result in a data transit through other countries, without the awareness of the sender. This is the case, for example, of cloud services in which ISPs' (Internet Service Providers) are often placed in different countries from that in which the service user resides. It should be also considered that the most direct involvement of individuals in cross border data transfers – due to the development of new technologies and business models for personal data processing – is accompanied by a substantial increase of the connected risks caused by misuse of conferred data, which expose the fundamental right of personal data protection to more serious breaches. It will suffice to consider the cases in which a cross border data transfer happens with

[1] General Agreement on Tariffs and Trade (30 October 1947) 55 UNTS 187.
[2] Marrakesh Agreement Establishing the World Trade Organization (15 April 1994) 1867 UNTS 3.
[3] Kuner (2011) 10.
[4] International Data Corporation, *Worldwide Semiannual Big Data and Analytics Spending Guide* (IDC, 2016).

the tacit intent to circumvent legal boundaries provided by the country where data subject resides.

Finally, it is necessary to consider the significant transformation of the geographic factor: while geography and territoriality are still key factors in the application of rules on data protection, they have become less important under an economic and technological point of view. Many enterprises, in fact, structure and base their operations on business lines rather than geography. This new way to operate is supported by the current technology which allows cross-border data transfers regardless of national boundaries[5].

Definitional Uncertainties

The examination of the phenomenon of cross-border transfers of personal data is plagued by a number of definitional uncertainties. For example: could the IP address be considered as personal data? The answer is not obvious at all, because it will be different depending on the data protection regime considered[6]. The possibility of accessible personal data over internet could integrate an international transfer?

It is a fact that *omnis definitio in iure civili periculosa est*, but it is nevertheless necessary to outline boundaries of the interpretation and application of the considered phenomenon. The DPD[7], which is highly considered thanks to its primacy in defining a general framework on data protection, does not provide, however, a specific definition of transfer of personal data. In this regard, art 25, para 1 merely shows that it is possible to transfer data already processed and to be processed in a third country where they are sent.

The ECJ has provided a significant elucidation on the concept of data transfer in the *Bodil Lindqvist* case[8]: it has made clear that the inclusion of personal data in a page of a website does not constitute a proper transfer by the EU to a third country, for the mere fact of making this information accessible, through an internet connection, to recipients that are physically located outside the EU. Otherwise, in fact, if an online publication of file was considered as a transfer within the meaning of the DPD, it should be considered directed to all those third countries in which there are the technical means to allow the access to the web page through internet connection. As a result of that, any data transfer would require the overall application of the DPD within a number of States (or even within all the Countries). This, however, is certainly not the effect desired by the legislature[9].

[5] Kuner (2011) 11.
[6] Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] OJ C89/4, Opinion of AG Campos Sánchez-Bordona.
[7] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (Data Protection Directive).
[8] Case C-101/01, *Sweden v Bodil Lindqvist* [2003] ECR I-12992.
[9] Poullet (2007) 149 cited by Piroddi (2016) 174.

Legal Systems Compared

The regulation of cross-border data transfers is primarily designed to prevent a transmission across national borders which could result into a circumvention of the legal limits imposed by the country of origin on personal data protection. Nevertheless, in some cases such regulation is reduced to a mere attempt to harmonise[10].

To avoid such evasive manoeuvres, the applicable law to transnational transfers is – in most instances – that of the country where the data subject is based. This is a clear expression of the 'extraterritoriality'[11] of rules on data protection, in other words, data protection rules can be applied to a specific data processing even if data are transferred across national boundaries. It is important to highlight that, however, rules on applicable law, as well as those relating to jurisdiction, have often blurred boundaries generating numerous practical problems. It is common that data subjects are not placed in a position to determine with certainty which of the applicable law applies to a given data processing, or which the competent national authority in case of breaches is[12].

The regulation of cross-border data transfers depends on different legal and cultural traditions. It differs, therefore, depending on the country or region of the data's origin. For example, in some countries or regions (e.g. European Union) rules on data protection are legally binding because the rules are intended to protect fundamental human rights[13], while in others the bedrock have to be found in the attempt to realise the economic benefits of electronic commerce (e.g. Asia Pacific Economic Co-operation) [14].

Traditionally among European countries there is a dual trend: on the one hand there is the tendency to transpose in writing these kinds of rules, a prerequisite for the application of sanctions and compensation; on the other hand, the tendency to provide for additional procedural mechanisms for the effective implementation of such legislation. Attitude, this confirmed by the DPD, provides for the establishment of supervisory authorities – with investigative and surveillance functions in the field of personal data protection – in each member state. Nevertheless, it is about procedural mechanisms that are not always shared by non-European legislative experiences, much less by the Convention 108/1981[15]. For these considerations, the risk that data transfers to third countries could turn into an expedient designed to circumvent legal restrictions stated by the country of origin is more than just potential, enough to induce lawmakers to provide for stricter rules on it.

It is furthermore considered that while some regulations about cross-border data transfers have a 'geographically-based' approach, in certain cases they are rather to make data exporters guarantor of the continuity on the

[10] Kuner (2011) 24.
[11] Poullet (2007); Svantesson (2014); Svantesson (2013); Resta (2016) 32
[12] Kuner (2011) 25.
[13] Bassini & Pollicino (2016).
[14] Kuner (2011) 7.
[15] Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [1981] ETS 108 (Convention 108/1981).

protection of personal data transferred to other entities, without the geographical position can have an influence on this[16].

From the Convention 108/1981 to the GDPR

The DPD is an important step forward in comparison to the Convention 108/1981 which relates to the protection of personal data in transnational transfers. The above makes, in fact, a balancing operation between the maintenance of a minimum standard of protection and the respect of the European principle of free movement of personal data[17].

However, the need of uniformity within the Union, as well as the need to adapt regulation which, despite recent interventions, dates back more than twenty years ago, led to the approval of the GDPR[18] repealing the DPD.

Within both DPD and GDPR there is the aim to state the free movement of data, essential for the realization of the European Digital Single Market. In fact, numerous provisions of the European data protection legislation are dedicated to the data transfer and declined in different forms of transmission, communication and diffusion. Ordinary precautions tend to tense up if those transfers involve third countries, in order to consider the possibility that those countries would not provide the same level of protection of personal data recognised by the EU. Consequently, the European Commission had to make a suitability assessment in the light of predefined indexes defined by both the DPD and the GDPR[19].

The principal aim of the European legislation on data protection is to provide to the individuals adequate safeguards in relation to the way in which their data are processed. This is an objective which is normally reached thanks to the combination of the data subjects' rights and duties of data processors and controllers[20], but it also usually faces significant difficulties when different systems are involved in the processing operations[21].

The combination of rights and obligations set by the DPD is not the simply result of the implementation of those already stated by the Convention

[16] Kuner (2011) 7.
[17] Modafferi (2015) 46.
[18] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 (General Data Protection Regulation).
[19] The lack of an adequacy decision, however, does not involve the necessary inability to transfer data, as importers and exporters are allowed to take further measures of lawfulness of data processing (e.g. binding corporate rules and standard contractual clauses), to ensure that the transfer does not reduce the level of protection, or, more surprisingly, circumvents the limits set by European legislation.
[20] Frosini (1995) 21.
[21] Article 29 Working Party, *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive* (WP 12, 1998).

108/1981, in turn not dissimilar to the OECD Guidelines of 1980[22] and the UN Guidelines of 1990[23]. In light of the above, it can therefore be affirmed that a high degree of consensus in relation to the content of rules on data protection extends far beyond the Union's member states[24].

The fellow feeling and the declaration of common principles do not determine, however, the need of uniformity on the data protection standards required by different national laws. In fact, beyond the abstract statement of principles, the effective application of the latter must be considered. Consequently, the evaluation of the level of protection provided by a specific third country must take into account not only the content of rules designed to protect personal data, but also (*rectius*, especially) the overall legal system in force in a specific third country in order to ensure their effectiveness.

The Value of Data

In relation to the economic value of data, it is usual to talk about 'data-value cycle' as a sequence of phases from 'datafication' to decision making: this process, evidently, is not a (linear) value chain, but a value cycle that involves feedback loops at several phases of the value creation process (see Figure 1)[25].

Figure 1. *Data Value Cycle*

Source: Organisation for Economic Co-operation and Development 2015

The first phase is 'datafication and data collection', which refers to the activity of data collection through the digitization of content and monitoring of activities, including those offline (e.g. through sensors): the huge amount of data processed constitute the so-called 'big data' (second phase). The latter, in particular, can be exploited through the 'data analytics' (third phase): once processed and interpreted, big data are typically useless considering that they

[22] Organisation for Economic Co-operation and Development, *Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data* (OECD, 1980).
[23] United Nations, *Guidelines concerning Computerised personal data files* (UN Doc A/RES/45/49, 1990).
[24] See also Frosini (2015).
[25] OECD (2015).

do not offer *prima facie* any clear information. The information accumulated over time converges in the 'knowledge base' (fourth phase): where the learning machine is involved, the base knowledge reflects the state of the learning system. The last phase is the 'decision making'. The value of data is mainly reaped at two different moments: first when data are transformed into knowledge, and then when they are used for decision making. These decisions lead to new and different data and, therefore, give boost to a new data value cycle.

Data as a Capital Good

Data are neither a consumer good, nor an intermediate good. In most cases, data can be classified as a capital good. Unlike consumer goods, intermediate and capital goods are used as inputs to produce other goods. Consumer goods are, instead, the end result of this production process. In addition, as data are a non-rival capital, they can in theory be used simultaneously by multiple users for multiple purposes as an input to produce an unlimited number of goods and services.

Capital goods consist of any tangible assets that an organization uses to produce goods or services. They do not exhaust their function as a result of their use, as for intermediate goods. This does not mean that data cannot be discarded after they have been used, given the costs of storage.

Furthermore, being a capital good does not mean that data do not depreciate like capital goods, whose value declines «as a result of physical deterioration, normal obsolescence or normal accidental damage». In the case of data, depreciation is more complex because it is context dependent. A number of factors can affect the value of data, in particular: the accuracy and the timeliness of data.

Moreover, data can depreciate in value when they begin to lose their relevance for a particular intended use. There is thus a temporal premium that is motivated by the real-time supply of data.

For business data there are fully fledged economic assets[26], *per se* freely tradable and whose transfer is essential for the development of the international electronic trade. Academics, indeed, consider the information, i.e. data, as an expression of a specific economic value which allows, those who own it, to generate profits otherwise not (or unlikely) achievable[27].

Nowadays data have a central role in the global economic landscape (from being driver of the commercial strategies to act as the main subject of business activities) and represent, in essence, a form of capital[28]. But they imply, albeit to a lesser extent, a 'regulatory cost'[29] for economic actors, as such potentially

[26] Giannone Codiglione (2011) 4-5 Dir inf 911, n 8. See also Arrow (1962); Litman (2000); Motti & Pardolesi (1991); Resta (2005); Rodotà (1995); Zencovich (1993).
[27] Arrow (1962) 614–615. On the big data phenomenon see also Mattioli (2015).
[28] Gorz (2003).
[29] Giannone Codiglione (2015) 910. On privacy costs see also Grossman (1982); Mantelero (2007).

productive of drawbacks for businesses in terms of competitiveness, especially (and a fortiori) under cross-border data transfers. Consider, for example, the competitive advantage of European companies compared to the US ones following the lapsing of the Safe Harbour regime[30], in relation to the costs that they would have to withstand - without a new assessment of adequacy - to make compliant to the European rules their cross-border data transfers[31].

Conclusions

The European rules on data protection, in its new formulation, consider data protection and privacy as fundamental rights, in line with the provisions of articles 7 and 8 of the Charter of Fundamental Rights of the EU. Albeit correct in principle, this qualification is likely to deprive data subjects of the right to freely negotiate with data controllers and processors. The rules on the consent, moreover, deprive them of the possibility of 'selling' their data for goods or services: nevertheless, such a sell takes place, indeed, every day, if we consider the numerous cases in which, in order to take advantage (for example, of a free Wi-Fi, or an app), users are forced to confer to the suppliers their personal data.

If personal data are considered as economic goods, they should be 'bartered' with greater freedom by data subjects, allowing them to exercise a negotiating power so far limited by severe rules on data protection. This happened thanks to the European rules for customers' protection, even then it was desirable the enactment of a regulation that could bridge the huge gap between data subjects (data sellers) and data controllers (data purchasers).

In this way, the current legislation other than imposing strict boundaries on companies, does not increase – as it should – the negotiating power of data subjects, more and more affected by the dominance of data controllers and processors.

References

Arrow, K.J. (1962). 'Economic Welfare and the Allocation of Resources for Invention' in Richard R Nelson (ed.)*The Rate and Direction of Inventive Activity: Economic and Social Factors*. Princeton University Press)

Bassini, M. & and Pollicino, O. (2016). 'La Carta dei diritti fondamentali dell'Unione europea nel reasoning dei giudici di Lussemburgo' in Giorgio Resta & Vincenzo Zeno Zencovich (eds.) *La protezione transnazionale dei dati personali. Dai "Safe Harbor Principles" al "Privacy Shield"*. Roma TrE-Press

[30] Commission Decision 2000/520/EC of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council 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 [2000] OJ L215/7 (Safe Harbour regime). Repealed by the ECJ case C-362/14, *Maximillian Schrems v Data Protection Commissioner* [2015] OJ C398/5.

[31] Giannone Codiglione (2015) 910. On the 'purposes of general interest' see also Pchwartz (2013); Bignami (2007).

Bignami, F. (2007). 'European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining' in 48 *B.C.L. Rev*. 48:609

Frosini, T.E. (2015). *Liberté Egalité Internet*. Editoriale Scientifica

Frosini, V. (1995). 'La libera circolazione dei beni e dei servizi informatici nel mercato comune europeo' in [1995] 1 *Dir inf*. 21

Giannone Codiglione, G. (2015). 'Libertà di impresa, concorrenza e neutralità della rete nel mercato transnazionale dei dati personali' (2015) 4-5 *Dir inf*. 910-911

Gorz, A (2003). *L'Immatériel. Connaissance, valeur et capital*. Galilée

Grossman, G.S. (1982).'Transborder Data Flow: Separating the Privacy Interests of Individuals and Corporations' in *NW. J. Int'l.L. & Bus.* 4:1

Kuner, C. (2011). 'Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future' (OECD Digital Economy Papers No 187, OECD Publishing, 2011)

Litman, J. (2000). 'Information Privacy/Information Property' in *Stan. L. Rev*. 52: 1283

Mantelero, A. (2007). *Il costo della privacy tra valore della persona e ragione d'impresa*. Giuffré.

Mattioli, M, (2015). 'Disclosing Big Data' in *Minn. L. Rev*. 99:535

Modafferi, F. (2015). *Lezioni di diritto alla protezione dei dati personali, alla riservatezza e all'identità personale.* Lulu.

Motti, C. & Pardolesi, R. (1991). 'L'informazione come bene' in Giorgio De Nova (ed), *Dalle res alle new properties*. Franco Angeli Edizioni

Organisation for Economic Co-operation and Development, Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (OECD, 1980)

Organisation for Economic Co-operation and Development, *Data-Driven Innovation. Big Data for Growth and Well-Being* (OECD Publishing 2015)

Piroddi, P (2016). 'I trasferimenti di dati personali verso Paesi terzi dopo la sentenza Schrems e nel nuovo regolamento generale sulla protezione dei dati' in Giorgio Resta and Vincenzo Zeno Zencovich (eds), *La protezione transnazionale dei dati personali. Dai "Safe Harbor Principles" al "Privacy Shield"*. Roma TrE-Press

Poullet, Y. (2007). 'Transborder Data Flows and Extraterritoriality: The European Position' in *J. Int'l. Commerc. L. & Tech.* 2:141

Resta, G. (2005). *Autonomia privata e diritti della personalità*. Jovene.

Rodotà, S. (1995). *Tecnologie e diritti*. il Mulino

Schwartz, P.M. (2013). 'The Eu-U.S. Privacy Collision: A Turn to Institutions and Procedures' in *Harv. L Rev.* 126:1966

Svantesson, D.J.B. (2013). 'Extraterritoriality in Data Privacy Regulation' in *Masaryk U. J. L. & Tech*. 7:87.

Svantesson, D.J.B. (2014). 'The Extraterritoriality of EU Data Privacy Law. Its Theoretical Justification and Its Practical Effect on U.S. Businesses' in *Stan. J. Int'l. L*. 50:53

Zeno Zencovich, V. (1993). 'Informazione. Profili Civilistici' in *Digesto civ*. 8:420

Cases

Case C-582/14 *Patrick Breyer v Bundesrepublik Deutschland* [2016] OJ C89/4, Opinion of AG Campos Sánchez-Bordona

Case C-101/01, *Sweden v Bodil Lindqvist* [2003] ECR I-12992

Documents

Article 29 Working Party, *Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive* (WP 12, 1998)

Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data [1981] ETS 108 (Convention 108/1981)

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31 (Data Protection Directive)

General Agreement on Tariffs and Trade (30 October 1947) 55 UNTS 187

International Data Corporation, *Worldwide Semiannual Big Data and Analytics Spending Guide* (IDC, 2016)

Marrakesh Agreement Establishing the World Trade Organization (15 April 1994) 1867 UNTS 3

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1 (General Data Protection Regulation).