June 25, 2016

The Human Right to Privacy and Personal Data Protection: Local-to-Global Governance in the Digital Era

2016 Research Project
Human Rights Working Group, Law Schools Global League

Preparatory document for LSGL Academic Conference
Northwestern Pritzker School of Law, July 19, 2016

Prepared by:

Prof. Amnon Lehavi, Interdisciplinary Center (IDC) Herzliya (chairperson)
Prof. Pierre Larouche, Tilburg University (co-convener)
Prof. Matej Accetto, Católica Global School of Law
Dr. Nadezhda (Nadya) Purtova, Tilburg University
Dr. Lior Zemer, Interdisciplinary Center (IDC) Herzliya

1. Introduction

The right to privacy is increasingly enshrined in constitutional and human rights instruments, and in some cases, a specific right to the protection of personal data is also included. At the same time, privacy and personal data protection are under a challenge in the digital era, due in particular to the worldwide proliferation of internet-based communications that are notoriously difficult to police; the rise of data-hungry applications like search engines, targeted advertising platforms or social networks; and the use of various methods of online surveillance by both private and governmental entities. The alleged borderless nature of digital technology leads to a complicated set of normative and policy questions. These queries relate not only to the adequate scope of substantive balancing between the individual interest in privacy and the potential interest of other private users, commercial entities, and governments in data disclosure, but also to questions of jurisdiction and governance. The dilemma is thus not only one of *how* (or *how far*) should privacy and personal data be protected, but also one of *who* should be in charge of establishing and enforcing the governing legal norms.

This preparatory document for the 2016 LSGL academic conference focuses on the current situation in Europe, both within the 47-member Council of Europe and the 28-member European Union.[1] The focus on Europe derives from major recent developments in rulemaking on balancing the interest in privacy with disclosure of personal data. However, these developments offer lessons that have a more global impact. This is due not only to the transnational effects of recent arrangements such as the recently signed "Privacy Shield" pact between the European Union and the United States, but moreover, to the ways in which such substantive dilemmas invoke aspects of the proper scale of regulatory and legal governance, moving from local to global.

The analysis of the current state of personal data protection in Europe and beyond is offered through the perspective of the various institutional actors that are involved in the process of designing and enforcing the legal instruments pertaining to data protection. Section 2 studies the role of EU legislative institutions. Section 3 reviews the role of supranational courts, in particular the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECHR). Section 4 investigates the position of national legislatures and regulators. Finally, Section 5 examines the role of private actors in rulemaking and enforcement of privacy rules.

2. EU legislative institutions

This section has two parts. Section 2.1 outlines the previous data protection legal landscape in the EU and the case for the reform. Section 2.2 focuses on the implications of the new regime for the institutional dynamics at the EU level.

2.1 Setting the stage: Data protection law in the EU prior to Regulation 2016/679

Prior to the current reform, the contours of European data protection law could be found in the following legal sources within the framework of the Council of Europe and the EU:

[1] This document was essentially written before the result of the June 23, 2016 British referendum to leave the European Union, and it does not therefore address the anticipated results of the British exit from the EU.

- The *European Convention on Human Rights (ECHR)*: although not explicitly including a specific right to the protection of personal data, this right has been found to be contained in the scope of the right to private and family life, home and correspondence (Art. 8 ECHR). See more on this in Section 3 below.
- The *Council of Europe (CoE) Convention No. 108*: a 1981 CoE Convention was the first binding international instrument on data protection law and it remains an important document, with all EU Member States being parties to it. Following the 1999 amendments, the CoE Convention also allows for accession by the EU, which has been in negotiation over the past few years, with the Commission enjoying an observer status.
- *EU law:* the initial cornerstone of EU data protection law was, and until 2018 still remains, Directive 95/46 (*Data Protection Directive*), supplemented by further legislation (e.g. Regulation 45/2001, Regulation 1049/2001, Directive 2002/58 and Directive 2006/24). With the entry into force of the Treaty of Lisbon, both the Treaty (TFEU) and the Charter of Fundamental Rights (CFR) also introduced provisions of EU primary law dealing explicitly with data protection rights.

It should come as no particular surprise that these instruments have been showing their age and struggling to keep up with the changing reality of data processing, in particular:

- advances in technological capabilities for the collection, transfer, and processing of personal data;
- implications of globalization on increased data flows across jurisdictions; and
- reconsideration of data protection concerns and legislation in light of competing interests, such as access to personal data by law enforcement agencies.

In the EU context, it is also relevant to note that the 1995 Data Protection Directive was adopted as an internal market measure, aiming to reconcile fundamental rights concerns for protection of personal data with the interest in free movement of such data within the internal market.

Over the recent years, there were a number of developments and concerns, which showed the (new) challenges of data protection and the struggles of the old regime in meeting them:

- The need to (re-)appraise data protection as a fundamental right, both as a concept (could it develop as a subset of the right to privacy or should it be given stronger autonomous foundation?) and in reconciling it with competing rights. Such rights may include freedom of expression (including media rights, and freedom of the arts and science), access to (public sector) documents, protection of property, and interests, such as the need of access to data for security and law enforcement purposes). This also resulted in developments such as the "right to be forgotten" recognized by the ECJ in *Google Spain* (following a logic similar to ECtHR's decisions in *Rotaru v. Romania* (App. No. 28341/95) and *M.M. v. UK* (App. No. 24029/07)) (See Section 3.1 below).
- The cross-border application and the globalization of data processing. The regime under the 1995 Data Protection Directive struggled to define both the scope of application (witness the delicate interplay between the "territorial" and "extra-territorial" triggers in Arts 4(1)(a) and 4(1)(c)) and applicable law (hesitating between the "country of origin" and the "cumulation" approach), which was ill-suited to the digital age. This is evidenced, for instance, by the considerations on the "use of equipment" condition and issues of applicable law in the Article 29 Data Protection Working Party opinions on cookies, search engines, and SWIFT. It was also shown by the controversies surrounding international agreements such as the "passenger name records" (PNR) agreements or the "safe harbor" principles allowing for processing and transfer of personal data to the US, the latter invalidated by the ECJ in C-362/14 *Schrems* (See Section 3.1 below).
- The need to reconcile data protection concerns with the security interests in surveillance and access to relevant data by law enforcement, among other things resulting in a controversial Data Retention Directive (Directive 2006/24) that was annulled by the ECJ in C-293/12 and C-594/12 *Digital Rights Ireland*.

The reform, surveyed in Section 2.2 below, aimed at addressing these challenges and other concerns, and explicitly listed the following objectives:

- strengthen individuals' data protection rights, including a revisit of the area of police and judicial cooperation in criminal matters, and more generally, institutional bolstering to improve their enforcement;
- clarify, facilitate and equalize the internal market dimension;

– unify, clarify and simplify the procedures for international transfer of personal data.

The Commission proposed the new legislation in January of 2012. Most importantly, it proposed to replace the 1995 Directive with a comprehensive regulation as the cornerstone of EU data protection law. After almost four years of negotiations among the EU institutions, the text of the new General Data Protection Regulation (GDPR) was agreed in December of 2015 and formally adopted in April 2016, and will apply from 25 May 2018.

2.2 Implications of the new regime for the institutional dynamics at the EU level

There are a number of institutional implications of the new data protection regime. This subsection focuses on three aspects of the changes in the institutional roles:

– new legislative and regulatory dynamics;
– new policy/monitoring dynamics; and
– new enforcement dynamics.

2.2.1 The new legislative dynamics: Delegated and implementing acts

Apart from the substantive reform to EU data protection law, GDPR is also an important testing ground for one of the important law-making changes introduced by the Treaty of Lisbon. This refers to the distinction between the "legislative acts" (adopted by the ordinary or special legislative procedure by the Council and/or Parliament, see Art. 289 TFEU), "delegated acts" (to be adopted by the Commission to "supplement or amend certain non-essential elements of the legislative act", see Art. 290 TFEU) and "implementing acts" (to be adopted by the Commission (or exceptionally by the Council) where uniform conditions for implementation are needed, see Art. 291 TFEU).

This change is notable for two reasons. First, it introduces a new dynamics and hierarchy of legal acts where no formal division existed before (except for the "implementing" powers referred to by former Art. 202 EC). Second, it replaces the old comitology system with the involvement of committees of national experts in regulatory matters (with four different procedures and important powers) with a weakened new system of comitology limited to

implementing acts. Taken together, the two changes may signal a new shift in interinstitutional dynamics between the Commission and the Union legislators, the Council and the Parliament, and give an incentive to the Commission to push for a greater use of the "non-legislative" legal acts in EU legislation.

That much can be evident from the text as well as the legislative history of GDPR. In its initial 2012 proposal (COM(2012) 11 final), the Commission envisaged no fewer than 26 delegated acts[2] (as well as numerous[3] implementing acts). Following its first reading of the proposal, the European Parliament in 2014 (P7_TA(2014)0212) already proposed halving this number.[4] In the final version of the text, the number of delegated acts envisioned is much smaller still – GDPR only envisages the adoption of delegated acts by the Commission in two cases: in defining the icons to be used in informing data subjects of the intended processing of their data (Art. 12(8)) and in specifying the requirements for data protection certification mechanisms to be encouraged as a means of demonstrating compliance with GDPR (Art. 43(8)). This dramatic decrease (which to a slightly lesser also took place with regard to implementing acts)[5] is worthy of further evaluation.

2.2.2. The new policy/monitoring dynamics: European Data Protection Board

In addition to supervisory authorities set up by Member States, the 1995 Data Protection Directive set up an independent expert body at an EU level, the so-called Article 29 Data Protection Working Party. It has been composed of representatives of the national supervisory authorities delegated by the Member States, a representative of the EU supervisory authority (the European Data Protection Supervisor (EDPS)) and a representative of the Commission. It has

[2] With provisions for them found in Arts 6(5), 8(3), 9(3), 12(5), 14(7), 15(3), 17(9), 20(6), 22(4), 23(3), 26(5), 28(5), 30(3), 31(5), 32(5), 33(6), 34(8), 35(11), 37(2), 39(2), 43(3), 44(7), 79(6), 81(3), 82(3) and 83(3).

[3] With provisions explicitly referring to them found in Arts 8(4), 12(6), 14(8), 15(4), 18(3), 23(4), 28(6), 30(4), 31(6), 32(6), 33(7), 34(9), 38(4), 39(3), 41(3), 41(4), 41(5), 42(2)(b), 43(4) and 55(10), and a further list in Art. 62 concerning the section on consistency.

[4] Its proposed rewording of Art. 86(2) summarized the story: "The ~~delegation of power~~ ***power to adopt delegated acts*** referred to in ~~Article 6(5), Article 8(3), Article 9(3), Article 12(5), Article 14(7), Article 15(3),~~ ***Article 13a(5),*** Article 17(9), ~~Article 20(6), Article 22(4), Article 23(3), Article 26(5), Article 28(5), Article 30(3), Article 31(5), Article 32(5), Article 336), Article 34(8), Article 35(11), Article 37(2),~~ ***Article 38(4),*** Article 39(2), ***Article 41(3), Article 41(5),*** Article 43(3), ~~Article 44(7), Article 79(6)~~ ***Article 79(7)*** , Article 81(3)~~,~~ ***and*** Article 82(3) ~~and Article 83(3)~~ shall be conferred on the Commission for an indeterminate period of time from the date of entry into force of this Regulation."

[5] Where the final version of the GDPR expressly refers to them in Arts 40(9), 43(9), 45(3), 45(5), 47(3), 61(9) and 67.

acted in the advisory capacity and has produced a number of opinions and recommendations trying to provide guidance on and a uniform interpretation of a number of unclear or controversial aspects of data protection law. For instance, in April 2016 it adopted its first opinion for the year on the EU–US Privacy Shield draft adequacy decision, prepared in the wake of the invalidation of the previous "Safe Harbor" agreement, wherein it welcomed significant improvements but stated strong concerns as regards lack of clarity, unregulated commercial aspects and large-scale access by public authorities to data transferred.

GDPR does not retain the Working Party but establishes a different, albeit similarly composed body, the European Data Protection Board (EDPB). The Board shall comprise the representatives of one supervisory authority from each Member State and (with certain voting limitations) the EDPS. The Commission will be allowed participation but without voting rights. GDPR (in Arts 68–74, in particular Art. 70) provides for a number of concrete tasks for the EDPB, which will comprise adoption of opinions, guidelines, recommendations, and best practices on varied issues concerning the implementation of and compliance with the Regulation.

It may also be added that, somewhat confusingly, the EU institutional framework already includes a number of supervisory bodies whose membership is also largely drawn from national data protection authorities and who are concerned with area-specific issues of data protection: the Joint Supervisory Authority of Schengen, the Joint Supervisory Body of Eurojust, the Europol Joint Supervisory Body and the Joint Supervisory Body of Customs.

It remains to be seen whether future reforms may bring about any operational streamlining of these various bodies and how far the role of the EDPB may be extended in the future. In any event, however, the EDPB may certainly play a defining role in the shaping of the new data protection regime and is a subject meriting further evaluation.

2.2.3. The new enforcement dynamics: One-stop shop and consistency

The third aspect brings together the various institutional actors and centres on another innovation in the Commission's proposal. This is the "one-stop shop" mechanism, whereby for each data controller or processor, the supervisory authority in the Member State of its "main establishment" would be designated as the lead authority for that controller and would be responsible for supervision of its compliance with the EU data protection law, in cooperation

with other authorities concerned. While this development was certainly welcome to the undertakings active in several Member States that were facing the possibility of parallel proceedings conducted by several national supervisory bodies, it raised other flags of concern, notably the possible lack of proximity and effective remedies for data subjects who would pay the price for data controller's or processor's convenience if they could no longer obtain redress through their own national supervisory authorities, a possibility for forum shopping and the potential problems in the event of a (positive) conflict of competence.

As with non-legislative acts, the initial proposal was heavily criticized, notably for the proposed strong role of the Commission in its initial proposal, which included the possibility of non-binding opinions of the EDPB alongside the power of the Commission not only to monitor decisions of national supervisory authorities but also to require their revision and even suspend their implementation. Both the Parliament and the Council significantly altered the proposed system, with the debates within the Council going so far as to question the legality of the "one-stop shop" mechanism.

Ultimately, a complex compromise mechanism was included in the final text of the GDPR, under which a lead authority is determined in the event of cross-border processing of data (Art. 56) but is required to cooperate fully with all other authorities concerned (Art. 60), while data subjects retain the right to lodge a complaint with their own supervisory authority (Art. 77). Moreover, the final version of the consistency mechanism provides for a much weaker role of the Commission and a bolstered role for the EDPB: the EDPB is to adopt opinions on draft decisions of lead authority in a number of cross-border circumstances (Art. 64(1)) or on other issues of general application in several Member States (Art. 64(2)). Even more importantly, the EDPB is to adopt binding decisions in the event of a reasoned objection to the draft decision by the lead authority, a competence dispute or when the competent authority fails to request or follow the EDPB opinion under Art. 64 (see Art. 65).

As with the other newly introduced aspects, it will only be possible to fully assess the operation of this new consistency mechanism after its implementation in practice. Nevertheless, as an important feature of the new regime that has been heavily debated and amended in the course of the legislative procedure, it already merits a more thorough evaluation.

3. Supranational courts and tribunals

As suggested in the Introduction, the right to privacy is increasingly enshrined in human rights conventions and other supranational legal instruments. Accordingly, supranational courts and tribunals, which are entrusted with interpreting and enforcing such legal norms, are playing a prominent role in giving substance to the human right to privacy, including in the specific context of protecting personal data. A number of key decisions rendered by supranational courts and tribunals over the past few years have challenged national rules and international agreements pertaining to the transfer of personal data within and across national borders. This substantial judicial oversight requires national legislatures and international organizations to reconsider the balancing of interests between the protection of privacy and legitimate goals of making such data available.

The following paragraphs briefly review the role of two supranational courts, the Court of Justice of the European Union (CJEU) and the European Court of Human Rights (ECHR), in devising the scope and limits of protecting personal data. This case law vividly demonstrates the intricate nature of processing and controlling personal data in the digital era, given the role of both private and public entities, and the often-overlapping layers of legal governance that should ensure adequate protection – from private user contracts to national, regional, and global governance of data protection.

Accordingly, the impact of this case law goes beyond the European Union and the Council of Europe, respectively. It deals explicitly with the transfer of private data outside of these jurisdictions, and more broadly, it serves as a prominent authority for legal debates about the proper protection of privacy of personal data across the globe. From a jurisprudential perspective, CJEU/ECHR legal standards of "proportionality" and "fair balance" between privacy as a human right and the public interest in transferring and processing data, may serve as a legal benchmark in the global setting.

3.1 Court of Justice of the European Union (CJEU)

This subsection reviews two seminal decisions rendered by CJEU, *Google Spain SL v. González* (2014) and *Schrems v. Data Protection Commissioner (Ireland)* (2015). These decisions were

anchored, inter alia, in the provisions of 1995 Data Protection Directive (see Section 2.1 above) and in Article 8 of the Charter of Fundamental Rights of the European Union ("EU Charter"), according to which:

Article 8: Protection of personal data

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.

Google Spain SL v. González dealt with a complaint by Costeja González, a Spanish citizen, lodged with the national Data Protection Agency against Google Spain SL, Google, Inc., and the Spanish daily newspaper *La Vanguardia*. According to the complaint, a google search of González's name led to two notices published in *La Vanguardia* in 1998 about an auction of his home for the recovery of social security debts. Stating that the proceedings have been since then fully resolved so that the reference was entirely irrelevant, González requested that the newspaper be required to remove the pages containing this personal data, and that Google be ordered to remove or conceal its search results that contain links leading to these web pages.

The court held, first, that the activity of a search engine such as Google should be classified as "processing of personal data" within the meaning of 1995 Data Protection Directive, and that the operator of the search engine is regarded as "controller" of such processing.

Second, the processing of such data is seen as carried out within the territory of a Member State when the operator of the search engine sets up in the Member State a branch or subsidiary in order to promote the sale of advertising space by that engine.

Third, as for "the right to be forgotten" – individuals have a right, under certain conditions, to ask search engines to remove links with personal information, when the information is excessive or no longer relevant, even if the publication itself is lawful. The right to be forgotten should be weighed, however, not only against the economic interest of the operator of the search engine, but also against the public interest in having access to that information, for example, when the person plays a public role.

The *Google Spain* case served as a further driving force for the enactment of the 2016 EU regulation on data protection, Regulation (EU) 2016/679, which repealed the 1995 Data Protection Directive (see Section 2.2 above). The regulation is intended to achieve substantial harmonization of data protection rules across the EU. As discussed in Section 2.2.3, it introduces a "one-stop-shop" for enforcement, meaning that business organizations, which are controllers or processors of data, will have to deal with only one national data protection authority, where their main business is located. Dealing with the various aspects of data protection, the Regulation explicitly introduces in Article 17 a "right to erasure" and respective balancing tests.

Alongside the Regulation, the European Parliament and the Council have also approved in April 2016 a new directive (Directive (EU) 2016/680) on the processing of personal data by competent authorities "for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties." Article 16 of the Directive includes a "right to rectification or erasure of personal data and restriction of processing." It allows Member States to adopt legislative measures that may restrict the rights of persons to be informed by data controllers of any refusal to rectify or erase their personal data. Such restrictions must, however, constitute "a necessary and proportionate measure in a democratic society with due regard for the fundamental rights and legitimate interests" of the persons concerned. The Regulation and Directive embrace, therefore, much of the jurisprudential framework of proportionality embraced by CJEU/ECHR case law.

Schrems v. Data Protection Commissioner (Ireland) dealt with a complaint by an Austrian citizen, a Facebook user, against the transfer of data from Facebook's Irish subsidiary to servers located in the United States. The Irish supervisory authority rejected the complaint on the ground that the EU Commission has decided in 2000, based on the US-EU "Safe Harbor" scheme, that the United States ensures an adequate level of protection of the personal data transferred. The CJEU held that the existence of a Commission decision, finding that a third country ensures an adequate level of protection of the data transferred, cannot eliminate or narrow down powers granted to the national supervisory authority under the EU Charter or the 1995 Data Protection Directive.

The Court further emphasized that it alone has the jurisdiction to decide that an EU act, such as a Commission decision, is invalid. The Court held that EU legislation permitting public

authorities to have access on a generalized basis to the content of electronic communications compromises the essence of the fundamental right to respect for private life. The same holds true for legislation that does not provide any possibility for an individual to pursue legal remedies in order to have access to personal data. Finally, the Commission's decision is invalid also because it does not have the authority to restrict the powers of the national supervisory authorities.

Following the *Schrems* decision, the European Union and the United States designed a new scheme, the "Privacy Shield," which is intended to impose stronger obligations on US companies to protect Europeans' personal data. It requires the US government to monitor and enforce these obligations more robustly, and cooperate more with European Data Protection Authorities. The scheme, as articulated in the proposal for a council decision (2016/0127 (NLE), dated April 29, 2016) goes beyond the setting of substantive standards for data protection to introduce forms for dispute resolution. First, a person is entitled to approach the data-processing company directly, which is required to respond within 45 days. In case of disagreement, the framework includes an alternative dispute resolution (ADR) mechanism free of charge. Data protection authorities in the European Union will work with the US Department of Commerce and the Federal Trade Commission to ensure that complaints by EU citizens are investigated and resolved without undue delay. As a last resort, the agreement includes international arbitration that renders an enforceable decision. The Privacy Shield framework received support from US companies but is facing objection from the Article 29 Data Protection Working Party. It is therefore unclear, at this stage, if and how the new framework will come into force. But the suggested framework already points to the influence of the CJEU, not only by increasing the level of protection of personal data, but also by setting up various cross-border mechanisms for dispute resolution all the way up to binding arbitration.

3.2 European Court of Human Rights (ECHR)

The ECHR has decided numerous cases concerning different aspects of the protection of personal data. This theme falls within the scope of private life as protected by Article 8 of the European Convention of Human Rights, according to which:

1. Everyone has the right to respect for his private and family life, his home, and his correspondence.

2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder of crime, for the protection of health and morals, or for the protection of the rights and freedoms of others.

Accordingly, the general standards of proportionality and fair balance have been invoked by the ECHR in a number of different contexts, from questions relating to data retrieved following surveillance, or the taking and retention of fingerprints or cellular materials and the storage of DNA profiles, and up to data protection in the digital era with specific reference to the Internet. This thick body of law had dealt both with the authority of public agencies to use such data for certain public goals, and with the "positive duty" of government to protect individuals from undue dissemination of data by other persons. For the former, see, e.g., *S. and Marper v The United Kingdom* (Dec. 4, 2008), in which the ECHR held that the police's refusal to destroy fingerprint records of persons acquitted in trial violates Article 8. For the latter, see, e.g., *Fürst-Pfeifer v. Austria* (May 17, 2016), in which the ECHR held that Austrian court's refusal to order a newspaper to pay damages to a psychiatrist for publishing medical information relating to her competence did not violate Article 8.

4. National legislatures and regulatory agencies

4.1 Background

As the previous sections have shown, the EU must act on the protection of personal data in order to give citizens back control over their personal data. European citizens enjoy a basic right to control their personal data under Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU). These Articles provide that everyone has the right to the protection of personal data concerning him or her.

The urge to remodel previous legislation on personal data protection was made stronger by a message sent by elected representatives of 16 EU member states, assembled in Paris for an inter-parliamentary meeting. The meeting, held on September 2014, assembled parliamentary delegations from 16 EU MSs that have called upon the EU to rapidly adopt the legislative package on the protection of personal data. In a joint declaration, representatives of the parliaments of Germany, Austria, Belgium, Croatia, France, Greece, Hungary, Lithuania, Luxembourg, the Netherlands, Portugal, the Czech Republic, Romania, the United Kingdom, Slovakia and Sweden, called on European legislators to urgently adopt the legislative package on the reform of personal data protection in light of globalisation and rapid technological changes that have redefined risks to privacy and the protection of personal data.[6]

Data protection has a strong cross-border dimension and a fundamental human value enshrined in basic legal instruments. For these and other reasons, a new regulation was adopted: Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 (see Section 2.2). The Preamble to the Regulation explains the cross-border effect of personal data protection**:**

> "The economic and social integration resulting from the functioning of the internal market has led to a substantial increase in cross-border flows of personal data. The exchange of personal data between public and private actors, including natural persons, associations and undertakings across the Union has increased. National authorities in the Member States are being called upon by Union law to cooperate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State."[7]

Regulations in sensitive areas, such as personal data protection, require, as many commentators provide, closer cooperation with national parliaments. As mentioned above, national parliaments of 16 Member States urged the Union's institutions to adopt the necessary regulation on the protection of personal data. This does not mean that they were part of the legislative process to a degree that sufficiently takes their views into account. True, the

[6] http://www.euractiv.com/section/digital/news/national-parliaments-raise-the-pressure-on-data-protection/

[7] Regulation Preamble sec (5). Sec 116 further provides that: "When personal data moves across borders outside the Union it may put at increased risk the ability of natural persons to exercise data protection rights in particular to protect themselves from the unlawful use or disclosure of that information

Regulation opens with the fact that it has been adopted only "After transmission of the draft legislative act to the national parliaments." However, as the following subsection will show, the role of national parliaments is overlooked.

4.2 National parliaments and the European Union

4.2.1 Before Lisbon

The vibrant scholarly debate on the democratic deficit in the European Union was mainly associated with the powers of the European Parliament. In reality, this concept is must wider and essentially contested. Various European institutions suffer from and contribute to the lack of democratic accountability in the Union. Amongst these institutions are national parliaments that were recently defined as the engines behind better integration. National Parliaments are embodiments of representative democracy at national level and hence important to the achievement of democratic legitimacy within the EU. As the European Commission stated in one of its communications: the European Parliament, and only it, is responsible to ensuring democratic legitimacy for the EU institutions' decisions, but, at the same time, "the role national parliaments will always remain crucial in ensuring legitimacy of Member States action in the European Council and the Council."[8]

While the competences of the EU have been enlarged and redefined over the past decades, the privileges of national parliaments have been substantially reduced in relation to European institutions. In other words, the establishment of the EU resulted in surrendering legislative competences of national parliaments to supranational EU institutions – a test case of a gradual process of de-democratization through integration. National parliaments were described as "victims" or "losers" in this process.[9] As one commentator once wrote, although the allocation of increased powers to the European Parliament cured parts of the democratic deficit within the Union, it must not be treated as a substitute to national parliaments.[10]

---

[8] Commission's Communication, "A blueprint for a deep and genuine economic and monetary union" COM (2012) 777.

[9] John O`Brien and Tapio Raunio, "National Parliaments within the Enlarged European Union: From 'Victims' of Integration to Competitive Actors?'" 8 (Routledge 2007)

[10] Adam Cygan, Accountability, Parliamentarism and Transparency in the EU: The Role of National Parliaments 6 (2013)

4.2.2 After Lisbon

The Lisbon Treaty reinforced not only the power of the European Parliament but also the powers of national parliaments. In this way the framers of the Lisbon Treaty aimed to enhance democratic legitimacy at the national level. After Lisbon, national parliaments are no longer peripheral to the development of European integration. Lisbon was the first Treaty to mention national parliaments in the text of the Treaty.[11]

For example, Article 12 defined their role as active contributors to the functioning of the European market. In addition, national parliaments are entitled to obtain information and play an important role in the monitoring of subsidiarity; protocol No 2 established the "early warning mechanism" which allows national parliaments a pre-legislative tool to intervene and challenge legislative proposals with the subsidiarity principle.[12] However, the warnings issued by national parliaments are of non-binding nature and come at a stage in the legislative process that is too late to make real impact. As such, this mechanism can be defined as a symbolic gesture rather than a workable regulatory mechanism. Moreover, arguably, the Treaty of Lisbon treats national parliaments separately from other European institutions (Art 13) and as such makes them secondary players[13] and with no formal constitutional role.

A recent inquiry into the role of national parliaments concluded its research with the following: "given the impact that EU activities have on national interests, scrutiny of EU matters is important, and is part and parcel of national parliaments' crucial role in protecting national interests and bringing democratic legitimacy to government decisions."

4.3 The role of national parliaments in the new regulation

The new Regulation recognises the fundamental role of national parliaments to achieving its objectives. Two examples reign supreme:

[11] For example, the Treaty of Maastricht mentioned the role of national parliaments by a non-binding Declaration No 13 [1992].

[12] Munro, White and Borjes, "Parliamentary Scrutiny of European Union Legislation" 35 (2016)

[13] Chalmers and Monti, European Union Law 42 (2008)

(1) Article 57(1)(c) provides that: "Without prejudice to other tasks set out under this Regulation, each supervisory authority shall on its territory…(c)advise, in accordance with Member State law, the national parliament, the government, and other institutions and bodies on legislative and administrative measures relating to the protection of natural persons' rights and freedoms with regard to processing."

(2) Article 59 on Activity Reports provides: "Each supervisory authority shall draw up an annual report on its activities, which may include a list of types of infringement notified and types of measures taken in accordance with Article 58(2). Those reports shall be transmitted to the national parliament, the government and other authorities as designated by Member State law. They shall be made available to the public, to the Commission and to the Board."

4.4. The case of Ireland and Belgium

That the protection of personal data is a sensitive issue was confirmed on June 2, 2016, when the EU and the US have signed the "Umbrella" agreement – the "Privacy Shield" that sets high standards for the protection of personal data transferred by law-enforcement authorities. The Agreement covers all personal data (for example names, addresses, criminal records) exchanged between the EU and the US for the purpose of prevention, detection, investigation and prosecution of criminal offences, including terrorism.

In the wake of new threats on European Member States, data protection has become a crucial issue. At the same time, individuals enjoy fundamental rights and these include the right to own or have access to their data. In order to enforce this right Member States of the EU have established, for example, Data Protection Commissions.[14] In Ireland, Data Protection Acts from 1988 and 2003 ensure that individuals have right of access to their data. For example, Section 3 provides that "An individual who believes that a person keeps personal data shall, if he so requests the person in writing-(a) be informed by the person whether he keeps any such data…" and Section 4 ensures access. In practice, the Data Protection Commissioner conducts investigations in light of breach of the Acts. For example, on June 13 2016 the Commissioner welcomed the successful outcome of prosecution proceedings taken by her Office against a

[14] See also Belgium Privacy Commission…

private investigator (PI), James Cowley, which concluded at Dublin Metropolitan District Court. In this case, Mr. Cowley was charged with sixty one counts of breaches of Section 22 of the Data Protection Acts in 2015. The charges relate to obtaining access to personal data without the prior authority of the data controller by whom the data was kept and disclosing that data to another person.

5. Private actors

5.1 Background

As already discussed above, the enactment of GDPR marked the first major reform of EU data protection legislation since the 1995 the Data Protection Directive. The GDPR replaces the Data Protection Directive, and brings major changes both to the substance of personal data protection law and to its procedural and institutional framework (see Section 2 above).

At the same time, the GDPR rests on the same basic assumptions as its predecessor. First of all, personal data protection (much like privacy) is seen as a matter of fundamental rights: Article 8 of the EU Charter of Fundamental Rights enshrines the right to the protection of personal data, and Article 16 TFEU provides a specific legal basis for the EU to act in the area.[15] These fundamental rights are deemed to filter down into private relationships, as reflected in the GDPR. Accordingly, it is assumed that personal data protection is not at the disposal of the parties (even if consent of the data subject plays a central role in the GDPR scheme) Secondly, the GDPR is primarily enforced according to a public enforcement model: the law is set out in a legislative instrument, and it is enforced by public authorities on behalf of the personal data subject as against the firm or organization collecting and holding the data (data collector). The GDPR develops that model further by strengthening the independence of the data protection authorities, their enforcement powers and their ability to cooperate across borders (on the model of comparable regulatory schemes in competition law or the regulation of network industries and financial services).

[15] The GDPR is based on the autonomous legal basis of Article 16 TFEU (concerned with data protection as such), whereas the Data Protection Directive was based on what is now Article 114 TFEU (internal market), so that data protection was harmonized – in theory – with a view to facilitate data flows between Member States.

In contrast, US law does not give a fundamental right dimension to the protection of personal data (or privacy) in the realm of private relationships.[16] Privacy and personal data are thus viewed primarily as goods that are at the disposal of private parties, and hence the development of the law in these areas is still left largely to self-regulation, with the State playing an advocacy and facilitation role. Similarly, the enforcement of these self-imposed norms (privacy and personal data policies) has been left largely to private actors, through contract, tort or property law.

At the risk of oversimplifying, one could draw the following matrix:

Privacy and data protection in private relationships	**EU**	**US**
Substantive law	Fundamental rights permeate the law	Self-regulation
Enforcement	Public	Private

The question then becomes whether the relationship between substantive law and enforcement is immutable, and in particular whether private enforcement is compatible with a fundamental rights perspective. The section aims to show that, when a fundamental rights perspective is taken, private enforcement can still play a large role and should not be ignored, especially against the backdrop of globalization.

5.2 The economics of information and privacy

In order to understand the position of actors in private relationships and their incentives, it is useful to look first at the economics of information and privacy. From an economics perspective, privacy and the protection of personal data can be seen as services over which parties may transact: these parties include individuals holding personal data, firms wanting to use that data,

[16] The US constitution has been interpreted to include privacy protection as against the State.

information intermediaries dealing in personal data, public authorities and privacy providers. From an analytical standpoint, the disclosure of personal data is neither categorically good nor bad for consumers and society. A simple property rights analysis cannot suffice to evaluate welfare effects of the disclosure of personal data. Classic market failures around information disclosure could prompt, but do not unambiguously justify public intervention. A more important concern is to which extent consumers are able to properly evaluate the costs and benefits of disclosing personal data. Empirical research points to a 'privacy paradox', a discrepancy between the stated preference for privacy protection and the observed behavior of customers; this provides a strong justification for a mandatory minimum requirement on privacy protection.

5.3 The limits of the public enforcement model

The public enforcement model used in the EU, however, suffers from a 'reality gap', or disconnect. In substance, it is not entirely adapted to data-centric business models (including Big Data), as opposed to business models where data processing is ancillary to a main business. And when it comes to enforcement, the public enforcement model cannot cope, because national Data Protection Authorities lack resources, and jurisdiction is not always established clearly. The GDPR reforms address these issues but are unlikely to solve them.

5.4 The prospects for private enforcement under a fundamental rights model

Such disconnect is no reason to abandon the EU approach, in favor of self-regulation in the US style. Rather, privacy and data protection law be cast as a baseline for private actors, as a guide to private parties in their dealings on and around privacy.

Using that baseline, private activities can then be given a greater role in the enforcement and development of privacy and data protection law. This goes in two directions: below that baseline, private enforcement – via liability – can supplement public enforcement. Above that baseline, private incentives to offer contractual protection can and must be encouraged.

Both scenarios can be developed to explore how the law can be designed to exploit the possibilities offered by the actions of private parties in order to improve its enforcement.

As regards liability, simply relying on general principles of tort law may not be enough. It might be advisable to flesh out a specific liability regime for breaches of privacy and personal data protection, including the basis for liability (fault or risk) and defenses, as well as the use of collective redress mechanisms.

As regards contract law, the GDPR does leave room for codes of conduct, certification and trust seals. The range of instruments is thus not far from what has been developed in the US. Yet under the GDPR, these instruments are primarily conceived from a public law perspective, i.e. as private mechanisms complementing public enforcement. This might not be enough. When firms want to go beyond the baseline of protection, a properly functioning market is needed. This is where a strong data portability principle, coupled with competition law enforcement, can play a role. Public authorities should also play a more proactive and advocacy role in ensuring the success of codes of conduct, certification and trust marks, in order to mitigate well-known market failures related to information or decisions that are not widely observable, once firms start to offer superior privacy and personal data protection. It is up to both public and private entities to work together in order to ensure better data protection, alongside the proper balancing of other interests, in the global digital era.