The European Union as a Constitutional Guardian of Internet Privacy and Data Protection: the Story of Article 16 TFEU

SHORT SUMMARY

There is a wide perception that governments are losing control over societal developments, due to globalization and technological phenomena, which inhibit the effective protection of essential values in democratic societies. Examples are the Snowden revelations concerning mass surveillance by the National Security Agency of the United States, also on European citizens, as well as the difficulty of having control over the privacy policies used by big internet companies, in a big data environment.

This study discusses privacy and data protection as essential values in democratic societies, which are subject to the rule of law. The EU Treaties have granted the Union a widely formulated role in ensuring effective protection of these fundamental rights of the individual, by means of judicial review, legislation and supervision by independent authorities. Hence, the imperative of protection is laid down at the constitutional level, empowering the Union to play its role as constitutional guardian of these two fundamental rights.

More precisely, Article 16 TFEU, read in connection with Articles 7 and 8 of the Charter of the Fundamental Rights of the Union, lays down the tasks of the EU in relation to privacy and data protection as fundamental rights for individuals. Article 16(1) TFEU and Articles 7 and 8 of the Charter specify the right to data protection which the EU should guarantee, ultimately under control of the Court of Justice, Article 16(2) TFEU empowers the EU legislator to set rules on data protection, and, finally, control should be ensured by independent authorities (under Article 16(2) TFEU and Article 8(3) Charter).

Article 16 TFEU gives the EU a specific mandate to ensure data protection, in addition to the general responsibility of the Union – and of the Member States where they act within the scope of EU law - to respect the fundamental rights laid down in the Charter. The Charter determines that where the EU acts, fundamental rights should be respected. Article 16 TFEU lays down that the EU shall act in order to ensure the fundamental right to data protection.

The mandate under Article 16 TFEU is broadly formulated and gives the Union – in principle – the power to act, and make a difference. This is a subject where the EU can act successfully, by addressing a problem with a global scale and which is technologically difficult. This is also essential for the EU itself in a time where the support for an EU which is more than a common market is fading. This perception of loss of control is probably even stronger in areas where the European Union is the central actor.

This specific mandate of the EU in respect of privacy and data protection is the subject of this study. The study analyses the contributions of the specific actors and roles within the EU framework: the judiciary, the EU legislator, the independent supervisory authorities, the cooperation mechanisms of these authorities, as well as the EU as actor in the external domain. The legitimacy and the effectiveness of the EU and of the operation of the actors and roles within the EU framework are important perspectives for this analysis.

General conclusions

This analysis shows that successful use of EU powers under Article 16 TFEU can be made, in conformity with the requirements of legitimacy and effectiveness. It also shows that ambitious approaches are needed, in view of the huge challenges in the information society.

The success of the EU in exercising its mandate under Article 16 TFEU is essential for individuals whose fundamental rights are at stake. It is also essential for our democracies which are subject to the rule of law. Moreover, if the Union can successfully deliver upon its ambitions under Article 16 TFEU and is capable to effectively contribute to the respect of the rights to privacy and data protection, this will give legitimacy to the mandate under the same article and in a wider context raise the trust in the EU (and indirectly, in national governments).

The perspective of this study is optimistic. The EU has an appropriate mandate to act in the area of privacy and data protection, with tasks attributed to the judiciary, the EU legislator and the independent data protection authorities, in principle without restrictions. The mandate also enables a successful cooperation of the data protection authorities and for the EU as such to operate in the international domain.

This optimistic perspective is also based on the strong position of Europe in the international domain, based on what has been called the "Brussels effect".[1] Law can make a difference in an information society provided that the available instruments are used in an intelligent manner. Moreover, the European Union is capable to deliver upon its ambitions laid down in its general constitutional structure, and in particular in Article 16 TFEU.

The success of the EU in the exercise of its mandate under Article 16 TFEU depends on the way the EU manages to reconcile the requirements of legitimacy and effectiveness. A successful exercise of the EU mandate in the domain of privacy and data protection could show the capabilities of the EU to protect fundamental rights in a global environment. This is a domain where not only law, but also the EU, by exercising its mandate in a successful manner, can make a difference.

This study argues that Article 16 TFEU could benefit from an understanding of the fundamental rights to privacy and data protection as such and in their relation to other fundamental rights which takes the changed environment of internet into account. Since, in an internet environment, all processing of personal data potentially affects the privacy of an

[1] The Brussels Effect, Anu Bradford, 2012, Northwestern University Law Review Vol. 107, No. 1

individual, it makes no longer sense to consider privacy and data protection as separate fundamental rights. On the contrary, these rights are part of one system. Furthermore, the right to data protection does not include a right to prohibit processing; on the contrary, it is a right to fairness.

Moreover, on the internet, privacy and data protection, on the one hand, and other fundamental rights, on the other hand, increasing collide, whereas, at the same time, the protection of fundamental rights becomes increasingly complicated. Against this background, a simple taxonomy of fundamental rights is proposed, enabling to differentiate in the level of protection, depending on the nature of the right.

The Court considers in its case law the need to compensate the perceived loss of control over personal data, enabled by the current legislative instruments on data protection and in particular Directive 95/46. The EU legislator works towards the adoption of a comprehensive and up to date legislative framework for data protection, bringing important innovations. The Treaties recognise the essential role of the control by data protection authorities with a high degree of independence, as confirmed in the case law of the Court. The authorities and their cooperation structures play an essential role in the development of data protection in the European Union. This role will be further developed in the new legislative framework. Finally, the EU plays an active role in the international arena, through the contributions of the various actors and roles under Article 16 TFEU.

Specific findings, focusing on the various actors and roles

Article 16 TFEU provides a strong mandate to the EU and ensures that privacy and data protection fall by definition within the scope of EU law. The high ambitions of the EU resulting from this mandate should compensate for the presumed lack of control on internet. The EU is not the sole guardian of privacy and data protection on the internet. Also the Member States have a role. The executive federalism should not adversely affect the harmonised level of protection.

An appropriate exercise of the mandate under Article 16 TFEU contributes to the EU's social legitimacy and can also be an element of the enjoyment of EU citizenship. EU action should also be legitimate vis-à-vis the Member States. Effective exercise of the mandate gives the EU output-legitimacy. Bridging the gap between principles of privacy and data protection and practice requires an appropriate choice of legislative arrangements, strengthening the various (public) actors and roles under EU law, as well as involving the private sector and leaving the final responsibility with governmental actors.

This study includes a number of ideas on the involvement of the various public and private actors in the governance of internet privacy and data protection. The study recommends elaborating these ideas and developing a strategy for this involvement, clearly describing the responsibilities of the various actors.

In recent years, **the Court of Justice** played an important role in promoting privacy and data protection, also taking into account the impact of the information society. Two judgements in 2014, *Google Spain and Google Inc*, and *Digital Rights Ireland and Seitlinger* are the best illustrations of a court, taking privacy and data protection serious. The recent *Schrems* ruling confirms this line.

This study does the following recommendation, to base the scrutiny of fundamental rights in an internet environment on a simple taxonomy. This taxonomy of fundamental rights is structured as follows:

a. Non-derogable or absolute fundamental rights, corresponding to the rights included in Title I of the Charter, entitled dignity;
b. Rights with a huge impact on the human dignity, but not qualified as non-derogable, such as privacy an d data protection;
c. Social, cultural and economic rights. Further categories include: principles in the Charter (as meant in Article 51(1) and 52(5) thereof), the fundamental freedoms of the Treaties, relating to free movement, the undefined species of public and general interests.

As far as **the EU legislator** is concerned, the study mentions five directions for the EU and the Member States to regain control. First, the existing legal instruments for privacy and data protection should be interpreted in a way, taking the changed circumstances into consideration; second, the legislative arrangements should be adapted to the new circumstances; third, the changed relation between the public and the private sector should be addressed, by recognizing a closer involvement of the private sector in the implementation of the law without questioning the final responsibility of government; fourth, the EU and the Member States should focus their interventions on essential components of privacy and data protection, for pragmatic reasons and for jurisdictional reasons; fifth, the EU and the Member States could reconsider the main principles of data protection, in order to adapt these principles to the changed circumstances, however without giving up on the need for protection of individuals. This fifth direction is for the long term, if only because the main principles of data protection are laid down in EU primary law.

The contribution of the EU legislator plays a key role in regaining control. A regulation is the appropriate legislative instrument, also for the public sector.

Data protection as a right to fair processing requires that the legislator gives effect to the core elements of data protection, mentioned in the Charter. The focus in the General Data Protection Regulation (GDPR) is the adaptation of legislative arrangements to the new circumstances. One thing the GDPR explicitly omits, is addressing the principles or values of privacy and data protection as such.

This study recommends developing a strategy for the legislator on how to regain control, based on the five directions mentioned above and focusing on the impact of the internet on the main principles of data protection. On the long term, this strategy could result in the re-thinking of the principles or values of privacy and data protection.

An essential part of the enforcement of EU data protection law is assigned to expert bodies, which are primarily **the independent data protection authorities (DPAs)** of the Member States. These DPAs are independent public authorities with a variety of roles: ombudsmen, auditors, consultants, educators, policy advisors, negotiators and enforcers[2]. In short, not only the mandate of the EU under Article 16 TFEU is broad, but so is the mandate of the DPAs within the EU and the Member States.

The embedding of the role of DPAs in primary law gives them constitutional status under EU law. This study qualifies the DPAs as a new branch of government, in the theory of Vibert.[3] DPAs do not derive their power from the other branches of government, as agents vis-à-vis a principal. By contrast, they are competent to supervise these other branches of government, the traditional *trias politica*. This new branch of government could be instrumental in restoring trust, if the authorities are completely independent and operate within a context of checks and balances. The DPAs should act within the limits of their competence in accordance with requirements of independence, effectiveness and accountability. Similar requirements are developed for good governance of agencies

This study proposes that a model for good governance for data protection authorities be developed. This model is inspired by the LITER Good Agency Principles[4], aiming at making agencies work better.

This study presents three models of **cooperation of DPAs**: horizontal cooperation of DPAs, a structured network of DPAs and cooperation within a European DPA. These three models compose a layered structure for an independent, effective and accountable control on EU data protection.

At present, the control on the compliance of data protection rules is not centralized at the EU level. Although considerations of effectiveness plead in favour of a uniform and harmonized approach of the control, this does not mean that centralization of the control would be the preferred option, at least not in the immediate future. Centralization of the control is also not favoured in any of the contributions of the EU institutions in the legislative process in the GDPR.

The study recommends elaborating the layered structure, as structure for a better governance of control on data privacy and data protection in the EU. This layered structure is not meant to centralize essential parts of the decision making by DPAs to the European level, but to ensure that where the European level is involved in the control on data protection rules, appropriate standards are in place.

[2] The Governance of Privacy, Colin J. Bennett and Charles D. Raab, 2003, Ashgate Publishing, at 109-114.
[3] F. Vibert, The Rise of the Unelected, Democracy and the New Separation of Powers, Cambridge University Press 2007.
[4] A. Ottow, Market & Competition Authorities, Good Agency Principles, Oxford 2015, mainly Chapter 3.

The EU as an actor in the external domain should take responsibility for globalization, based on the claim that EU values have a normative strength and are universally applicable. The EU has global power through the legal standards representing these values.

In order to ensure effective protection of individuals on the internet, the preferred strategy should be the unilateral strategy, aiming at exporting EU values in the international domain. The EU could thereby use facilities offered by the Council of Europe, such as the possibility that non-European countries adhere to Convention 108. As part of this strategy on practical level, bridges should be built with likeminded countries.

In addition, the bilateral strategy should be explored, focusing on mutual recognition, standardisation processes or enforcement cooperation, based on the communalities between the systems, but also accepting the differences. The OECD could possibly play a role.

In the long term, a UN-Treaty would ensure best protection (the multilateral approach). The EU should take initiatives in order to facilitate the adoption of such a Treaty, with the ambition to achieve a minimum standard of data protection.

Finally

For the short term, the General Data Protection Regulation means a significant step for data protection in the European Union, with relevance for all actors under Article 16 TFEU.

The General Data Protection Regulation does however not solve all weaknesses in the system. It remains to be seen whether, in the long term perspective, the Regulation suffices. Subjects that in any event require further action on the longer term are:

- The adaptation of the substantive principles of data protection.
- The fine-tuning of the role of the Member States under Article 16 TFEU.
- The centralization of the supervision of global internet companies

These subjects should be further explored in academic research in the coming years.