GEM STONES

AGORA© FORUM POLICY BRIEF

GEM-STONES AGORA© FORUM, MARCH 2020

PRIVACY IN THE DIGITAL AGE

WHAT ROLE FOR PUBLIC AND PRIVATE ACTORS?

Guillaume Beaumier

SUMMARY

The protection of privacy is an issue of particular importance in the growing digital economy. While being a hot topic long before the rise of the Internet and connected devices, the development of increasingly powerful data collection and processing methods has brought it back to the forefront of public debates globally. Next to new public laws being adopted, self-regulatory programmes developed by industry have been promoted since the mid-1990s. How both public and private rules have contributed to the governance of data protection is in that context a key question. Based on in-depth analysis of all self-regulatory programmes adopted in the United States and Europe since 1995 as well as interviews with key informants in both jurisdictions, this policy brief suggests:

- As a general rule, self-regulatory tools have almost always been spurred by public actions. Private forms of regulation should thus not be seen as a replacement, but a complement to public laws that often need to be supported by public actors.
- The assumed flexibility and adaptiveness of self-regulatory tools is generally quite limited. The creation of new legal obligations is the exception rather than the rule.

Privacy sticker in Lyon, France

- Self-regulatory tools can however be useful in clarifying how broad obligations can be applied in specific economic sectors.
- Despite mitigated results in promoting compliance with data protection laws, self-regulatory tools can be useful and help ensure that similar rules are followed in various jurisdictions at the same time.
- The European Union can thus benefit from continuing to proactively engage with industry to promote the development of self-regulatory tools as it tries to ensure that the GDPR is applied.

INTRODUCTION

In recent years, the protection of privacy has taken a center stage in public debates globally. With the rise of increasingly powerful digital technologies, many countries have grappled with the question of how to guarantee a certain level of control over how personal information is collected and used. Next to the risks of misuse of information by private companies (i.e., Cambridge Analytica scandal), many voices now caution against the risks of seeing a rise in discrimination or biased decisions based on the increasing use of artificial intelligence technologies trained to analyze the personal data of thousands of people.

In Europe where privacy is broadly viewed as a human right enshrined in the European Convention on Human Rights (1950) and the Charter of Fundamental Rights (2000), this notably led to a significant revision of data protection rules, which culminated with the adoption of the General Data Protection Regulation (GDPR) in 2016 by the European Union (EU). Long recognized has a global leader in privacy debates, the replacement of EU's two-decades old Data Directive has had consequences in all corners of the world. While the United States (US) still debate the need to have a comprehensive privacy law at the federal level, the updated rules have influenced the protection of privacy in various jurisdictions. Countries like Brazil and India that adopted new privacy laws in respectively 2018 and 2019 significantly incorporated many provisions and guarantees found in the GDPR. In Canada, the privacy law is similarly currently being reviewed to align itself more closely with it. Europe's market size and regulatory capacity increasingly seems to give the ability to shape privacy rules worldwide.

Next to these adoptions of new or revised legislations, private actors have also contributed to the regulation of privacy notably through the adoption of various self-regulatory tools. Taking varying forms (e.g., guidelines, best practices, codes of conduct, certification schemes, voluntary labels), these self-regulatory instruments aimed to set out rules on how to collect and use personal information by and for industry players. While particularly promoted in the US, they also played a consequential part in the evolving European privacy system. As a matter of fact, the GDPR nowadays give them an even greater role than the Data directive used to. In addition to provide for the creation of codes of conduct by specific industry sectors to help them specify how data protection rules should apply to their specific area of activities, the GDPR foresees that industry could also create certification schemes to demonstrate their compliance with it. Moreover, both codes of conduct and certifications are now considered to acceptable guarantees for data transfer to non-European countries.

This reliance on private or self-regulatory tools raises a number of questions for the governance of privacy as well as other issue-areas (i.e., environment) where such type of regulatory instruments are increasingly being developed and used. If for critics this form of regulation is fundamentally non-democratic, it is considered by the European Commission has an important way to make its rules more successful. In effect, the promotion of private regulation has become a full part of the Better Regulation Agenda of the EU, a reform programme aiming at making EU regulations "more priority-driven, evidence-informed, transparent and effective."

It is especially assumed that self-regulatory mechanisms can both bring flexibility and help in the implementation phase. Faced with evolving problems and technologies, self-regulatory are first considered to be able to more easily adapt themselves. They do not need to go through the entire process of changing laws, which can be quite cumbersome. The negotiation of the GDPR took for example almost four years to complete after it was first announced. Meanwhile, self-regulatory tools can also help ensure that rules established by governments are actually followed. The addition of certification schemes in the GDPR is specifically aimed at this. The extent to which self-regulatory tools achieves these two aims is however debatable.

KEY FINDINGS

Based on the analysis of all publicly available self-regulatory tools adopted in the EU and the US since 1995, few observations can be made. First, it is important to note that few self-regulatory tools were purely adopted by the industry. As opposed to the idea sometimes professed that private companies can create and enforce rules for and by themselves, most self-regulatory tools were created in collaboration or with the help of public actors in both the EU and the United States. This is perhaps most important to note in the United States where the official position has almost always been that the private sector should lead in the regulation of the digital economy. The Federal Trade Commission in collaboration with other federal agencies has however always been proactive in ensuring

that private companies respected the rules that they set up for themselves as well as pushed some business associations (e.g., Better Business Bureau) to create self-regulatory programmes.

In Europe, the adoption of codes of conduct by private actors has constantly been influenced by the work of data protection agencies (DPAs). It was actually foreseen in the Data Directive of 1995 that the European Union should promote the adoption of such types of private initiatives and could even approve them. This notably happened once with the code of conduct prepared by the Federation of European Direct and Interactive Marketing (FEDMA). In recent years, DG Connect has also been particularly active in bringing private actors from both the industry and civil society to work on codes of conduct for specific sectors (e.g., health and cloud computing). While not directly influencing the development of these programmes, it played an important role as orchestrator.

Overall, the creation of self-regulatory tools appears to be thriving when the public actors are thus involved. Many representatives interviewed in this research remarked that the significant costs of preparing and operating self-regulatory programmes often limited the desire of the industry to do it alone. The collaboration with public agencies was thus essential in spurring private actors to get involved. This could simultaneously help in alleviating risks of democratic deficit associated with private regulation. At the same time, this raised questions over the supposed flexibility associated with it. Developing private programmes between public and private actors often end up in a long process that can quickly become similar to the adoption of public laws. The adoption of FEDMA's code of conduct in Europe took for example four years and recent codes on health applications and cloud computing are still not formally adopted.

With that being said, it is also noteworthy that even in the United States where the involvement of public actors is still lighter than in Europe self-regulatory tools were never as flexible as its proponent argue it can be. Over the years, various industry rules were amended and changed, but it is rarely substantial. Major changes in effect seem to mostly occur after new public laws are adopted. This tends to show that while self-regulatory programmes can indeed create new obligations for private companies, they most often specify obligations that are already present in public laws. By specifying legal obligations, private actors can still play a significant role as in that process they can sometimes make data protection rules evolve in light of technological progress. They can also use recommendations made by data protection agencies or other public agencies on how to best apply the existing rules.

In doing so, they contribute to ensuring that the enforcement of public rules remain effective. Private actors can in effect play a particularly useful role at the enforcement stage. It is indeed clear that public actors in both the United States and Europe have difficulties to deal with all the privacy violations happening nowadays. The severity of the problems that can come with data breaches or misuse of personal data also make important that mechanisms are put in place to ensure that data protection rules are respected before any problems occur. Over the years, it is however source of concern that the respect of self-regulatory programmes by private companies has often been problematic. The Safe Harbor programme negotiated between the United States and Europe, which relied heavily on self-regulatory tools, was in effect criticized and, in the end, terminated for its lack of enforcement. It again stands out that self-regulatory programmes work best when public actors act as backstop.

These risks should nonetheless not lead to the conclusion that self-regulatory programmes have no value. As mentioned above, they can help enforcing public laws by helping individual sectors to apply broad data protection rules. Moreover, it was also observed that they can be useful in ensuring that the same rules are applied in different jurisdictions. One key issue in our connected world is that personal data can quickly cross national frontiers. Recognizing this, the GDPR also applies to the processing of personal data of Europeans that can occur outside of Europe. While the adoption of the GDPR has led various countries to change their national laws as previously indicated, there remains discrepancies between the protections guaranteed in various jurisdictions and it is still hard to ensure that the same data protection rules are always followed. One way through which it can be done is precisely self-regulatory tools as it is recognized in the GDPR and by the European Data Protection Board.

POLICY RECOMMENDATIONS

- The European Commission should continue to support financially and logistically the development of codes of conduct and certification schemes.
- While doing so, the European Data Protection Board should particularly aim to ensure that these self-regulatory tools include real and constraining compliance mechanisms and that civil society groups are involved during their creation.
- To help diffuse its rules to other jurisdictions, the European Commission could also invite foreign or international business associations that while contributing to the development of European self-regulatory tools could learn and be socialized to European rules.
- To ensure that these mechanisms are followed, the European Commission could financially support civil society groups that can notably lodge complaints in the name of European citizens under the GDPR for violations of data protection rules.

SUGGESTED READING

Braithwaite, J., & Drahos, P. (2000). Global business regulation. Cambridge (UK): Cambridge university press.

Bradford, A. (2020). The Brussels Effect: How the European Union Rules the World. Oxford (UK): Oxford University Press.

Farrell, H., & Newman, A. L. (2019). Of privacy and power: The transatlantic struggle over freedom and security. Princeton (NJ): Princeton University Press.

Newman, A. (2008). Protectors of privacy: Regulating personal data in the global economy. Ithaca (NY): Cornell University Press.

Pasquale, Frank. (2015). The black box society. Boston (MA): Harvard University Press.

Zuboff, S. (2019). The age of surveillance capitalism: The fight for a human future at the new frontier of power. London (UK): Profile Books.

Guillaume Beaumier is completing his thesis within the framework of an MSCA-funded GEM-STONES European Joint Doctorate between the University of Warwick (UK) and the Université Laval (CA).
guillaume.beaumier@gem-stones.eu

For permission to cite or reproduce any part of this publication, please contact the author.

Photo: @EV/Unsplash

More about the programme: www.gem-stones.eu

This research has received funding from the European Union's Horizon 2020 Research and Innovation programme under the Marie Sklodowska-Curie Grant Agreement No **722826**