한국언론학회
2018 봄철 정기학술대회

디지털 주권과 국가의 역할
Digital sovereignty and the role of the state

제1발제 :

Digital sovereignty and European personal data regulation

(디지털 주권과 유럽의 데이터 규제)

Bernard Benhamou
(디지털 주권연구소(Institute of Digital Sovereignty) 사무총장)

Korean Society for Journalism & Communication Studies

DIGITAL SOVEREIGNTY & EUROPEAN DATA REGULATION

PROSPECTS OF THE GDPR IN THE AFTERMATH OF THE CAMBRIDGE ANALYTICA CRISIS

Bernard Benhamou

Secretary General of the Institute of Digital Sovereignty

> *In recent years, we've seen conspiracy theories trend on social media platforms, fake Twitter and Facebook accounts stoke social tensions, external actors interfere in elections, and criminals steal troves of personal data… A legal or regulatory framework that accounts for social objectives may help ease those tensions.*
>
> Sir Tim Berners-Lee[1]

> *Surveillance is the business model of the Internet, we live in an era of « surveillance capitalism »*
>
> Bruce Schneier[2]

For several decades, European privacy regulations have been considered by the American technology industry as an inhibiting force for the development of digital economy. Five years after the Snowden's revelations on NSA's mass surveillance programs and after the recent Cambridge Analytica scandal, the international perception of European position on privacy has evolved. The threat of a systemic trust crisis caused by the unbridled dissemination of personal information is now a distinct possibility. Both for political and economical reasons, this is now a major concern for lawmakers and regulators. For Tom Wheeler, the former chairman of the american Federal Communications Commission, when it comes to privacy :

---

[1] Berners-Lee Tim, director of the W3C (Web Foundation, Mar. 2018) *The web is under threat. Join us and fight for it*

[2] Schneier B. (2015), *Data and Goliath*, New York, Ed. Norton & Company.

Bernard Benhamou
Institute of Digital Sovereignty
19 May 2018

« *The New World must learn from the Old World…*[3] »

Threats of Systemic Trust Crisis

Trust is the cornerstone of the development of the Internet ecosystem. Since data-driven companies (like Facebook or Google) have a primary business model based on profiling; cybersecurity threats and privacy issues could further erode users trust. A systemic collapse of users trust could have significant impact on the entire economic system. This could soon decide regulators to challenge « microtargeting » business models on both sides of the Atlantic. As Shoshana Zuboff[4], the Harvard Business School professor of business administration describes:

> Tech companies are gathering our information online and selling it to the highest bidder, whether government or retailer. In this world of surveillance capitalism, profit depends not only on predicting but modifying our online behaviour. How will this fusion of capitalism and the digital shape the values that define our future?

---

[3] *Congress is now considering bipartisan legislation that responds to the problem of Russian targeted political advertising on social media by adding the requirement, long applied to broadcast advertising, to disclose who is paying for their advertisements. But it addresses only a symptom of the problem of the extensive surveillance of Americans, not its root. The New World must learn from the Old World. The internet economy has made our personal data a corporate commodity. The United States government must return control of that information to its owners (…) The European regulation is powerful in its simplicity: It ensures that consumers own their private information and thus have the right to control its usage and that internet companies have an obligation to give consumers the tools to exercise that control. GDPR, for instance, require companies to provide a plain-language description of their information-gathering practices, including how the data is used, as well as have users explicitly "opt in" to having their information collected. The rules also give consumers the right to see what information about them is being held, and the ability to have that information erased.*
Can Europe Lead on Privacy? (New York Times, 1 Apr. 2018)
https://www.nytimes.com/2018/04/01/opinion/europe-privacy-protections.html

[4] Zuboff Shoshana (2018) The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (Ed. PublicAffairs)

Bernard Benhamou
Institute of Digital Sovereignty
19 May 2018

As several senators and congressmen stated during the hearing of Facebook CEO Mark Zuckerberg, the European General Data Protection Regulation (GDPR) could become a guide for future regulations on privacy beyond the European Union. If GDPR was at first considered as an industrial regulation tool, it is also dedicated to promoting European values and principles of control over personal data. Paul Nemitz, a director in the European Commission's justice department uses an interesting analogy between data protection and political ecology which eventually created an entire business sector[5]:

> It is probably true that in the future digital world, people will ask for more privacy protection and more protection of personal data rather than less. As it was with the Green movement, which started in Europe and which led European industry to enormous competitiveness but had resistance in the beginning in the '70s and '80s, it is very well possible also with data we will see the same trend.

On the opposite side of the privacy spectrum, the Chinese government plans to launch its Social Credit System in 2020. The aim of this new generation of social network is to judge the trustworthiness of 1.3 billion of Chinese citizens. The three digits 'rating' of each citizen will then affect their home, transport and even social circle…

New kinds of dissemination of even more sensitive data could soon have an impact on public opinions in democratic countries. As mass genomic technologies become widely available, they could be used as a tool for social control. For example, a bill of law (HR1313) currently under debate in the United States Congress aims to force employees to have genetic testing for health prevention purposes. The employees who would decline such tests could then face heavy penalties[6].

---

[5] Europe pivots between safety and privacy online (Christian Science Monitor, 18 Jan. 2015) https://www.csmonitor.com/World/Europe/2015/0118/Europe-pivots-between-safety-and-privacy-online

[6] Employees who decline genetic testing could face penalties under proposed bill (Washington Post, 11 Mar. 2017) https://www.washingtonpost.com/news/to-your-health/wp/2017/03/11/employees-who-decline-genetic-testing-could-face-penalities-under-proposed-bill/

Bernard Benhamou
Institute of Digital Sovereignty
19 May 2018

European new legal framework

In January 2017, President Donald Trump signed an executive order which stripped privacy rights from non-U.S. citizens[7]. This executive order could eventually nullify the EU-US Data Flows frameworks (also called *Privacy Shield*). This *Privacy Shield* is currently used by more than 1600 american companies and organizations. It allows the processing of European citizens personal data by american companies. But organizations like Digital Rights Ireland and French privacy groups have already launched actions before the Court of Justice of the European Union to annul the *Privacy Shield* (after the Snowden revelations, the previous agreement the *Safe Harbor*, has been overturned by the same Court in 2015).

After China, Russia… and for exact opposite reasons, the European Union could soon impose *Data Residency* rules for personal data of European residents. Personal data could not be transferred overseas and should be processed in the European Union. Even before the Cambridge Analytica scandal emerged, large companies like Microsoft and Amazon were investing heavily in building more data centers in Europe[8]. These preemptive measures could protect their future activities from possible evolutions of European regulations.

European norms and standards influence on next generations of technologies

Even more than the threats of cyberattacks, European member states have become aware of their vulnerability to technological developments over which they have little control. For Sigmar Gabriel, former German Federal Minister for Economic Affairs and Energy, European information technology companies must be able to develop their own norms and standards for digital technologies. It is increasingly important as these technologies have an

[7] TechCrunch 26 january 2017
https://techcrunch.com/2017/01/26/trump-order-strips-privacy-rights-from-non-u-s-citizens-could-nix-eu-us-data-flows/

[8] U.S. Tech Giants Are Investing Billions to Keep Data in Europe (New York Times, 3 Oct 2016)
https://www.nytimes.com/2016/10/04/technology/us-europe-cloud-computing-amazon-microsoft-google.html

impact on virtually all economic sectors and human activities. European member states can no longer accept a situation in which they have no sovereignty over their own essential informational infrastructures.

Regulation of the Algorithms

In the upcoming times, users control over personal information will not be the only needed aspect of the digital regulation. Since they will have impact on most aspects of our everyday lives, transparency of algorithms will be another key element of democratic societies. Those algorithms are already essential for large platforms (like search engines and social networks) and will be strategic for next generations of connected devices (like Artificial Intelligence algorithms used in conversational computers, medical devices or in driverless cars). As Frank Pasquale analyzed it in his book, The Black Box Society[9]:

> Demanding transparency is only the first step. An intelligible society would assure that key decisions of its most important firms are fair, nondiscriminatory, and open to criticism. Silicon Valley and Wall Street need to accept as much accountability as they impose on others.

The « Code » of these algorithms is currently opaque and unchecked by the citizens. As Pr Lawrence Lessig expressed in 1999: technological « Code is Law[10] » and the architecture of that code is becoming as important as the legal code of our democracies and thus must be under the control of citizens.

The Internet of Things: an even more political landscape

The Internet has become a crucial political object as it is already shaping multiples aspects of

[9] Pasquale Frank (2015) The Black Box Society (Ed. Harvard University Press)

[10] Lessig Lawrence (1999) Code & other Laws of Cyberspace (Ed. Basic Books)

our social, economical and political lives. The current evolution of technologies will establish the transformation from a mobile Internet to an "Internet of things" that will gradually connect every single object around us. Be it sovereignty, civil liberties or economic control, the political stakes of this "Internet of things" are already considerable. It will thus be necessary that this "Internet of things" be under the control of citizens. Data protection, security and confidentiality must be part of the architecture of digital services and connected objects. It must be considered not as an afterthought, but at design phase. *Privacy by Design* (and *Privacy by Default)* must be the rule in order to control if (and when) connected devices are allowed to «talk» about their users. Citizens must be able to control the way in which their personal data are used, and even the way in which these chips can be deactivated. A new right for the citizens in the era of the Internet of Things must be created: the right to the "Silence of the Chips".

Bernard Benhamou
Institute of Digital Sovereignty
19 May 2018