FONDATION ROBERT SCHUMAN

POLICY PAPER

European issues
n°484
18th September 2018

What the European personal data protection model shows us

Constance Bommelaer de Leusse
Lucien Castex

Hundreds of millions of people now use the Internet on a daily basis in many different ways: shopping, on-line banking, social network, etc. On the Internet they exchange an exponential amount of data, some of which is of an eminently personal nature. The dangers inherent to this are also growing and range widely from the unauthorised processing of data, to fraud and even to the manipulation of public opinion, which is endangering modern democracy. For all of these reasons, privacy and the protection personal data has become a European priority. A digital single market will not see the light of day if users do not have any trust in it.

I - A PROTECTION IN LINE WITH EUROPE'S ASPIRATIONS

The protection of personal data has rapidly become a central issue in Europe. This right was formalised in 1981 with the Council of Europe's 108 Convention, then in 1995 with the adoption of a first European directive. It is covered by the European Union's Charter of Fundamental Rights. Since 25th May 2018, the applicability of the General Data Protection Regulation (GDPR) has enabled the adaptation of protection to the most recent technological developments.

Criticised by other regional powers, who accuse it of compensating its lack of innovation via regulatory protectionism, Europe has distinguished itself through its choices that can be justified other than for economic reasons.

Indeed, the European model for protecting Privacy reflects a certain conception of mankind and society. The European Union aims to support a data policy that puts people's interest first. Hence it permanently tries to find a balance between the quest for innovation and the protection of its citizens. The sharing of competences in terms of the responsibility of the national, European and extra-European authorities is also a complex game.

Although the Internet is borderless by nature, the location of data and the exchange of personal data between States is geographical, which leads to questions regarding digital sovereignty. The European norm in terms of Privacy and free flow of data is put to the test in this respect. Bearing witness to this was the invalidation of the Safe Harbor agreement between the European Union and the USA by the European Court of Justice in 2015. It was replaced by the Privacy Shield in October 2017.

Tensions between regions of the world are also reflected in the shape of regulatory competition. The European authorities hope to protect their citizens and at the same time extend their economic influence. Aware that Africa and Latin America traditionally find inspiration in their example, they hope that the latter will adopt compatible rules so that they can remain privileged partners.

However, other regional powers are organising and preparing their own legal instruments. This is notably the case with the USA and the "Cloud Act" project, i.e. the Clarifying Lawful Overseas Use of Data Act, which involves access to data, stored abroad, an extra-territorial text that may bring with it the risk of interference. China has already chosen to be impermeable to any regulatory influence that might limit its digital independence. The country operates hermetically hosting a limited number of foreign operators with the obligation to locate data in China itself.

In this context, there is a danger of fragmentation of the digital space. Certain services based on other

continents might become unavailable because they do not comply with the rules of the user's country. With this trend the myth of an interconnected world might be coming to an end.

II - THE CHOICE OF STRENGTHENED, EXHAUSTIVE PROTECTION

From the protection of the citizen to the protection of his/her data

In 1995 the European Union introduced a legal framework via the **directive 95/46/CE** on *"the protection of individuals with regard to the processing of personal data and on the free movement of such data"*

The European Commission hoped to establish a uniform protective framework supporting the movement of personal data followed the opening of the borders. To quote former European Commissioner Viviane Reding in 2002, the aim was to *"boost the European economy"*. The spirit of the text aimed to protect individuals from the dangers that went with the development of the use and consolidation of on-line services, without suffocating the opportunities represented by this amazing market.

Today, the availability of the Cloud combined with massive processing capabilities and the power of artificial intelligence is enabling an ever more sophisticated use of data and personalised services. Simultaneously, consumers and citizens are more aware of the risks they run. With the Wikileaks and Cambridge Analytica scandals and the revelations made by whistle-blowers like Edward Snowden, they understand that the surveillance to which they may be subject is not just aimed at commercial ends but political ones too.

The recognition of a fundamental right

The right to the protection of personal data and the right to privacy are rights per se. The latter postulates what we might often call "the right to be left alone". Everyone *"has the right to the respect of his/her privacy."* In addition, secrecy of correspondence is also protected under criminal law which applies to the traditional postal letter to the e-mail.

The former, the right to the protection of personal data, targets all data regarding an identified or identifiable physical person. This means family names and first names and also videos or an IP address on the Internet. The processing of such data is regulated as is the collation, registration, organisation, storage, interconnexion operation and even the destruction of it.

Since 2009, the protection of personal data has been one of the European Union's fundamental rights. It was then that the outline of a new legal framework, the GDPR, emerged, which has been in force since 25th May 2018. Negotiations regarding this regulation extended over four years, from January 2012 to April 2016 and led to an overall reform of the legal framework of personal data protection. A two-year transition phase in terms of its implementation provided an opportunity to raise awareness and to empower European citizens, as well as those responsible for the processing of their data together with their subcontractors.

This regulation, which replaces the 1995 directive, is completed with a directive on the protection of personal data within the framework of police and judicial work. The role of national regulators, like the European Data Protection Supervisor (EDPS) which replaces the working group of article 29 at Union level has been extended. Greater cooperation between national and European regulators is indeed vital for a coherent and prospective implementation of the GDPR.

What changes with the GDPR

The GDPR implies that free, informed, positive consent by the Internet user has to be given, and lays down the fundamental principles of legality, trustworthiness and transparency in terms of data processing. The key principles of the 1995 directive remains valid: from the right to be informed on the use made of personal data collated, to the right to oppose and withdraw consent as well as access and rectification rights. The data controller, along

with the data processors, also have to declare any data leakage and take into account the protection of personal data as soon as a new service is conceived. He has to demonstrate that he is first and foremost a protector. Hence, there are no pre-ticked boxes on a website or tacit consent in order to be able to continue navigating.

The possibilities of disanonymisation, entangled sets of personal and non-personal data, likewise the development of indirect identification capacities, make the prospective design of data protection compulsory. The GDPR offers an approach based on risk management, which supposes the assessment of the impact of personal data processing and the adaptation of sanctions, in the event of the seriousness of the infringement not being considered.

Moreover, citizens' ability to act so that they can take back control over their data has been strengthened. Administrative sanctions, as well as the powers of the regulators have largely been extended.

Article 80 of the GDPR introduces a new European class action mechanism to bring to address any shortcomings in terms of data protection. It states that Member States can, under their national law, allow associations to exercise this right on behalf of those involved.

Article 82, with the recital 146, states that the data controller or the subcontractor must repair any damage caused by an infringement to the regulation that can be traced back to them, since data subjects involved must *"receive full and effective compensation for the damage caused"*, whether this is material or moral. This overlapping of national and European law lends the GDPR its strength. Indeed, it is up to Member States to opt or not for the right to compensation.

In conclusion, the GDPR introduces a balanced system, with a mix of cybersecurity and data protection. However, a holistic analysis commands to acknowledge the economic cost of its implementation, particularly for SMEs. Moreover, the flexibility given to Member States raises the issue of perfect compatibility among the data protection regimes across Europe. In the near future, it would be useful to specify the subjective notion of the data controller's legitimate interest, one of the legal bases of processing without consent. The means of implementing the duty of information on the part of the data controller must also be clarified. We should hope that the guidelines of the EDPS will, following the **WP29** (the group of European CNIL), provide details to these concepts.

Electronic communication data

This legal framework would not be complete if electronic communications were not included. Lex specialis of the GDPR, a draft European regulation regarding the respect of private life and the protection of personal data in electronic communications is being debated at present and should replace **directive 2002/58/CE**.

As it targets the protection of *"electronic communication"* confidentiality it tries to cover all communications: the traditional kind, as well as the electronic (OTT with Skype and Whatsapp), whatever the technology used. As the text stands the draft regulation would apply to cookies, metadata, as well as machine to machine communication.

The draft text aims to harmonise the different national legislations regarding electronic communications in the European Union so that they comply with the GDPR. This reflects a clear determination to help European Internet users trust the web by fostering practices which are respectful of their data. Hence, it is a difficult balance to strike between fundamental rights (limitation on tracking-walls, the need for a prior opt-in and up to the delicate question of fingerprinting) and the economic model of many digital services, particularly that of targeted advertising. This is what is at stake in the creation of a balanced digital single market for more than 500 million citizens.
In conclusion, the text should foster the principle of prior consent, again with the need to limit the exceptions, particularly of legitimate interest and further processing. Some issues are still pending however and deserve clarification. Indeed, should we not tighten up the confidentiality parameters of web

browsers and other software that enable electronic communications? And even improve the concepts of default protection, whilst leaving open the possibility of a fine, site per site configuration for example? And finally, shouldn't standards like *"Do not track"* be made compulsory?

III - FUTURE ISSUES

Despite these new regulations, Member States continue to reflect on the evolving needs for better data protection and privacy. Initiatives such as *"Data for Good"* or the organisation of international events like the UN's **Internet Governance Forum** (IFG) on 12-14 November demonstrate this dynamic.

These discussions should be taken as opportunities to question the Internet's economic model, notably from the point of view of competitive practices. If it appears that there are a limited number of players who abuse their dominant position on the market using methods that are not very respectful of private life, new standards might be necessary.

Europe's digital strategy

Last April, the European Commission presented its approach to countering on-line disinformation and tasked a panel of high-level experts on Artificial Intelligence (AI) to steer the work of the European AI Alliance. Data protection, notably those of a personal nature, should be central to this new instance. It will be based on the principles of limiting the collection of data and the length of time these can be stored.

With the massive deployment the Internet of Things (IoT) in European households, the rise of machine learning and machine-to-machine communication, these principles should continue to illustrate their relevance in the coming years.

Constance Bommelaer de Leusse
Director of Public Policy, ISOC Monde

Lucien Castex
Researcher, Université Sorbonne Nouvelle,
Secretary General, ISOC France

Retrouvez l'ensemble de nos publications sur notre site :
www.robert-schuman.eu

Directeur de la publication : Pascale JOANNIN