DIGITAL EUROPE

Europe and cyberspace – Data protection

Gregory VOSS

ABSTRACT

The development of computer technology raised concerns for the privacy of the individuals to whom data being processed relates. Soon European nations began adopting data protection laws to protect the privacy of individuals, eventually regulating what had become known as "cyberspace." To allow for the free flow of personal data within the European Union, while protecting the privacy of individuals, the regional block adopted EU-wide data protection legislation in 1995, which was then implemented in Member State law.

The lack of harmonization of Member State implementing legislation and the development of new technologies led to the adoption of a uniform EU law in the form of the General Data Protection Regulation (GDPR), which has had international impact. The GDPR develops further individual rights and continues cross-border transfer restrictions, while including clearer extraterritorial application when the personal data of individuals in the European Union are collected, thus recognizing that cyberspace does not end at borders.

Cyberspace and the Need for the EU General Data Protection Regulation ("GDPR")

The development of computer technology in the 1960s and 1970s raised concern among certain policymakers, computer scientists, and legal scholars about the potential harm to the privacy of those whose information was processed. Computers stored such information relatively cheaply and they could be used to easily find and retrieve the data. With the development of computer technology, storage capabilities increased, and the size of storage media decreased. Data on individuals coming from different sources could be linked, and this could cause privacy concerns, whether the information was held by governments or private organizations.

Governments soon realized that they had to regulate the use of computer technology to process information about natural persons. In the 1970s, European nations began adopting data protection laws in order to protect the privacy of individuals, under the right to privacy that is enshrined in the European Convention for the Protection of Human Rights and Fundamental Freedoms (1950). The first such law is that of the German federal region of Hesse (1970). Later, the Swedish Data Law (1973) was adopted, the German federal data protection law (1977) followed, with the French, Austrian, Danish and Norwegian data protection laws coming in 1978. These national and regional laws may be described as first-generation data protection legislation.

Initially, the Internet was seen as a zone of relative freedom—not only a place where users could communicate more or less anonymously, but also an area free from government regulation. This new area became known as "cyberspace," the online world formed by networks of computers and other internet-connected devices such as smartphones and tablets spanning the globe. Thus, cyberspace extends beyond national borders. However, as we have seen, governments eventually began to regulate cyberspace, as they did the physical world.

In order to avoid barriers to transfer of personal data within the European Union, the European Parliament and the Council adopted a proposal for an EU Data Protection Directive 95/46 (1995), which was then implemented in EU member state law, becoming what may be referred to as second-generation data protection legislation. While the main basis for the competence of the European Union to adopt such legislation was to remove barriers within the Single Market, both dimensions—the free movement of personal data and protection of

the right to privacy—were considered simultaneously. However, subsequently new technologies developed that had not been envisioned when the Directive was written, and there was found to be a lack of harmonization in the ways and means used by member states to implement the Directive. Thus, the European Commission proposed a law to replace it in 2012—the General Data Protection Regulation or "GDPR." The European Union had adopted the Charter of Fundamental Rights of the European Union (2000) and amended it in 2007. The Charter became legally binding after the entry into force of the Treaty of Lisbon (2009) and included a specific fundamental right to data protection. The GDPR is supplemented in the field of telecommunications by the ePrivacy Directive 2002/58/EC (2002), as amended by Directive 2009/136/EC (2009), which is currently subject to the legislative process on a Commission proposal for it to become a new ePrivacy Regulation.

Adoption of the GDPR in Context

The GDPR proposal was made at a time when economic relationships had changed as a result of the increasing availability at a reasonable price of personal computers and their connection to cyberspace. Businesses found that they could use this new cyberspace to further their commercial interests through direct distance selling referred to as e-commerce. An essential factor in e-commerce, access to the internet in the European Union increased from 64% in 2009 to 90% in 2019. The percent of individuals in the European Union engaging in e-commerce, defined as ordering goods or services online, increased from 20.4% in 2004 to an estimated 64.7% in 2020. European consumer spending over the Internet, which lagged behind that of the United States, was a mere $1 billion in 1998. However, over time European e-commerce revenue shot up and was expected to reach $465 billion in 2021.

Some businesses started collecting information about their users' purchasing habits and browsing history using small computer programs or files known as "cookies," which were introduced in 1995, and become known to public in 1996. These cookies were used for customer relationship management and shopping recommendations targeting the buyers' interests, and the ePrivacy Directive regulates their use. However, soon new ways of doing business by providing free services on the Internet were developed, which attracted users and made them accustomed to having access to content and services on a free basis. A key example of this is Google, founded in 1998, which initially offered its free search services. Yet, such commercial exchanges were not completely disinterested as the service providers attracted users, which allowed them to sell advertisements. Eventually, companies began collecting information on users, referred to in Europe as personal data, in order to use these data to offer personalized advertising or to create profiles on users. This allowed search, social media, and technology companies such as Google and Facebook to become online advertising powerhouses.

The United States (US) tech giants were generally not constrained in their home market by data protection legislation targeting their activities, other than when they published a privacy policy and then failed to respect it. The GDPR was seen as a way to level the playing field between EU companies and companies coming from other jurisdictions, such as the United States, without such protective legislation. Under the GDPR, a technology company not established in the European Union but for example, in the United States, would have to abide by the same data protection rules as an EU-established company when it offered goods or services to consumers in the European Union. Thus, in order to function properly the GDPR had to have what is known as extraterritorial effect, meaning that it had to apply to

companies located outside of the European Union's borders, but which collected personal data from individuals in the European Union, even if the processing of such data took place outside of the European Union. In such a way, the reality of the borderless nature of cyberspace was recognized.

The legislative process in the European Union was impacted by the revelations made by Edward Snowden in the summer of 2013 about mass surveillance programs of the US National Security Agency (NSA). Many US tech giants worked with the NSA to various extents. The atmosphere resulting from this disclosure allowed the European Parliament's committee responsible for the GDPR draft—LIBE (Civil Liberties, Justice and Home Affairs)—to overcome lobbying efforts and quickly agree on a version of the GDPR, which the European Parliament approved in plenary session, in first reading in March 2014. However, it took the Council of the European Union until June 2015 to establish its common position, and trilogue negotiations led to a political agreement among the Commission, the Parliament and the Council in December 2015. The GDPR was formally adopted in April 2016, entered into force in May of that year, and became applicable two years later on May 25, 2018, becoming, together with Member State implementing legislation, what may be called third-generation data protection legislation.

The Contours of the GDPR and Its Application in Cyberspace

The GDPR is an evolution of the EU Data Protection Directive 95/46 in one instrument—a regulation—which is generally applicable in all of the EU member states—unlike the case of a directive, for which Member States have the freedom to choose the form and the method of implementation into national law. Another earlier example of a regulation used for data protection purposes is Regulation 45/2001 which dealt with data processing by EU institutions and has been replaced by Regulation (EU) 2018/1725 on the protection of natural persons with regard to the processing of personal data by the EU institutions, bodies, offices and agencies ("EUDPR").

Data protection principles already existed in the EU Data Protection Directive 95/46, but have been further developed in the GDPR, and include requirements as to data quality, purpose limitation, data security, transparency about the collection and processing of their data toward the data subjects, rights of the data subject, accountability for respect of data protection requirements, and lawfulness and fairness of processing. Under the GDPR, data subject rights, which already included the right to access their data, the right to rectification of data, the right to deletion of data when no longer necessary for the purpose for which they were processed, and the right to object to processing under the Directive 95/46, now include the right to erasure ("right to be forgotten") and the right to data portability, as well.

The focus of the GDPR has shifted from the Directive 95/46's system of prior declarations for the processing of data to one of accountability, where controllers (which determine the purposes and means of the data processing) and processors (who process data on behalf of controllers, and according to their instructions), must be able to prove their compliance with the GDPR at any time to supervisory authorities. Under the GDPR, other new provisions include the requirement for most controllers (other than certain SMEs) to maintain a register of data processing activities, and many companies must now have a data protection officer ("DPO") who can assist in ensuring compliance. Furthermore, the GDPR makes reference to technologies such as biotech, location data, genetic data, and so on. In addition, the GDPR

has also established data breach notification requirements, which did not exist under Directive 95/46, and in the case of data protection violations the GDPR sets out potentially large administrative penalties, which are much more dissuasive than those under the Directive.

In order for the GDPR to become applicable to cases of processing of personal data, its scope requirements must be met. In the case of its material scope requirement, data must relate to a living individual, known as a "data subject." However, the GDPR does not apply when the household exception is applicable, that is when the data processing is carried out in a purely personal or household activity with no connection to a professional or commercial activity. Also, the GDPR does not apply to the personal data of deceased persons or to the data of legal persons such as companies. Furthermore, the GDPR also does not apply to data processing for matters involving law enforcement (the prevention, investigation, detection or prosecution of criminal offenses and the execution of criminal penalties), which are covered by Directive (EU) 2016/680, known as the "Law Enforcement Directive," which was adopted as part of a data protection legislative package including, and simultaneously with, the GDPR.

If the GDPR's material scope requirement is met, its territorial scope requirement must also be met in order for the GDPR to apply. The GDPR will apply if processing is carried out in the context of activities of an EU establishment, regardless of where the processing takes place. Furthermore, if a controller or processors targets sales of goods or services (even when no payment for them is made) to individuals located in the European Union, or monitors the behavior of such individuals, when such behavior takes place in the European Union, the GDPR will apply to the processing, even though the controller or processor is not established in the European Union. In such case, the controller or processor (other than a public authority or body, and in certain other cases where processing constitutes a low risk for the rights and freedoms of individuals) will be required to designate a representative in the European Union who may be addressed by the supervisory authorities.

Assuming that both GDPR scope requirements are met, companies and public operators other than EU institutions and bodies (covered by the EUDPR) that collect the personal data of data subjects located in the European Union, whether or not such individuals have EU citizenship, must have a legitimate basis under the GDPR to conduct the data processing. Examples of such legitimate bases include the data subject having given consent to the collection and processing of his or her data, the data being necessary for the performance of a contract to which the data subject is a party, among other bases.

Furthermore, in recognition of the fact that cyberspace does not stop at the European Union's borders, the GDPR continues a cross-border data transfer restriction that already existed under the Directive. This provides that data may be transferred (or exported) to a country outside of the European Union or to an international organization only if such country or organization has obtained a determination by the European Commission that it ensures an adequate level of protection of the personal data, failing which adequate safeguards must be provided. These adequate safeguards include the use of standard contractual clauses ("SCC") adopted or approved by the European Commission, binding corporate rules ("BCR") adopted by corporate groups and approved by the relevant competent supervisory authority, approved codes of conduct or certification mechanisms, and legally binding and enforceable instruments between public authorities or bodies.

In 2000, and then again in 2016, the European Commission issued adequacy decisions based on bilateral agreements with the United States establishing a framework for companies to self-certify adherence to framework principles intended to provide similar protection to data subjects as under EU law when their personal data are transferred to the United States. Each of those decisions was invalidated by the Court of Justice of the European Union ("CJEU"), in cases brought by the Irish High Court following complaints by an Austrian national name Maximilian Schrems. These cases involved Facebook, which transferred Schrems' personal data to the United States. There, the data could be accessed by public authorities for the purposes of surveillance under programs revealed earlier by Snowden, without the procedural guarantees provided under EU law. The first case ("*Schrems I*") involved the earlier US-EU Safe Harbor Framework, which was invalidated by the CJEU in October 2015. The second ("*Schrems II*") was actually a challenge to the use of SCC, but the CJEU took the opportunity to invalidate the successor to the Safe Harbor—the EU-US Privacy Shield—in July 2020. In 2021, negotiations were ongoing between the United States and the European Commission on a replacement for the Privacy Shield.

Importantly, the CJEU did not invalidate the use of SCC in *Schrems II* but conditioned their use on an assessment of the data importer's ability to respect the terms of the SCC, given the context of the legislation and practice of their home country. Certain trade law commentators have seen this as a "soft" data localization requirement, encouraging the storing of data in the European Union, in contrast to "hard" data localization requirements such as those found in Russia, China and in other countries. It is clear that using EU service providers to process personal data in the European Union simplifies the compliance efforts of companies, however there is no requirement that that they do this.

Not only does the GDPR regulate part of the activities of companies and individuals in cyberspace, including those in other countries who target goods or services at those in the European Union, but its influence reaches beyond borders as a sort of European soft power, through global standard-setting. What has been labelled "the Brussels Effect" by Professor Anu Bradford, affects areas where the European Union has established stringent rules regulating inelastic targets, such as consumer markets, and where there is a benefit for economic actors, such as multi-national enterprises, to adhere to one standard worldwide, rather than taking advantage of low standards is another jurisdiction through "forum-shopping." There may be an incentive to do so because of the size and wealth of the EU market. Once enterprises have adopted the higher EU standards internationally, the idea goes, they have an interest in lobbying other jurisdictions to adopt such higher standards to ensure a "level playing-field" with their competitors. Furthermore, this market-based power is complemented by normative power.

In the area of data protection, the GDPR is attractive as a single-legal instrument standard for regulating companies, individuals and public bodies, with the European Data Protection Board ("EDPB") providing guidance on the interpretation of its precise civil-law based text. It also benefits from multiple-language translations such as French, English and Spanish. As a result, many countries in Latin America, Africa and Asia, often with historical ties to European nations, have modelled their legislation after the GDPR and its predecessor (Directive 95/46), rather than copying the sectoral approach of the United States, for example. This diffusion of the EU model is spurred on by what has been referred to as treaty-based harmonization, which has resulted from EU institutional goals to export EU standards. The European Commission's inclusion of parallel discussions about data protection when they negotiate

new trade agreements, such as the agreement with Japan (2018), for example, helps achieve these goals. Furthermore, in June 2021 the European Commission approved an adequacy decision for transfers of personal data under the GDPR with existing free-trade agreement partner South Korea, and in 2017 the European Commission indicated that the countries of Latin America (especially the members of Mercosur) and India were also potential future targets of adequacy discussions.

Nonetheless, certain law and technology commentators assert that, because of regulation of personal data in the European Union, the region has fallen behind other blocs such as China and the United States in the development of new technologies such as big data, artificial intelligence and machine learning. The argument goes that regulation stifles innovation by entrepreneurs in these areas, and that it is more difficult for the European Union to create major "big tech" companies such as those found in the United States and China, as a result. Only time will tell if this is in fact the case or whether the other blocs will seek to temper their development of new technologies by the recognition of a fundamental right to data protection, the adoption of general data protection legislation, and the consideration of ethics relating to technology, as well.

BIBLIOGRAPHY

BRADFORD, Anu, *The Brussels Effect,* New York, 2020.

GONZ□LEZ FUSTER, Gloria, *The Emergence of Personal Data Protection as a Fundamental Right of the EU*, Cham, 2014.

LYNSKEY, Orla, *The Foundations of EU Data Protection Law,* Oxford, 2015.

VOSS, W. Gregory, "Cross-Border Data Flows, the GDPR, and Data Governance,' 29(3) *Washington International Law Journal* 485-531 (2020).

VOSS, W. Gregory, "European Union Data Privacy Law Reform: General Data Protection Regulation, Privacy Shield, and the Right to Delisting," 72(1) *Business Lawyer* 221-233 (Winter 2016-2017).

VOSS, W. Gregory, "Obstacles to Transatlantic Harmonization of Data Privacy Law in Context," 2019(2) *University of Illinois Journal of Law, Technology & Policy* 405-463 (Fall 2019).
