The GDPR three years later…

Marie-Laure Denis,
Conseiller d'État, president of CNIL

Abstract:
In force since 25 May 2018, the General Data Protection Regulation (GDPR) is, it is worth pointing out, one of the very few EU texts still being talked about three years following its adoption. Its application places Europeans on equal footing with international competitors and allows Europe to take a full place in the global digital economy. In fact, several countries have updated their regulations in line with EU regulations. Cooperation is a reality on our continent, and an EU legal doctrine is emerging. As statistics in France have shown, citizens massively exercise their rights when the latter are explained to them. The political and legal context in 2020 (exceptional in many regards) has led to a novel alignment of our interests in both data protection and industrial policy. The latter has to be placed at the service of an ambitious strategy in pursuit of digital sovereignty.

As the EU's General Data Protection Regulation (GDPR) celebrates its third anniversary on 25 May 2021, we have to admit that it is still a driving force at all levels.[1] It is on the political agenda and in the media worldwide. To evaluate what has been achieved, let us start by briefly recalling this regulation and the issues related to its operational success.[2]

The GDPR for building confidence in digital technology

A reminder of its principles

Since the invention of computer science, all spheres of society have become "digitized". Personal data are now a pillar of business, and firms are collecting ever more personal data to hone their information on customers and personalize products and services. The development of connected devices, profiling, control procedures and algorithms of all sorts, along with the increase in cyberattacks and the revelations from the Snowden affair in 2013, has made people aware of how necessary it is to better protect personal data.

Beyond the risks to privacy stemming from the poor management and insufficient security of personal data, some data processing techniques also carry real risks for freedoms, both individual and public. For instance, a disproportionate use of video- or cybersurveillance might place people in the situation of being nearly always controlled and set off reflexes of self-censorship.

The GDPR was not drafted in an ivory tower. After having conceptualized rights and freedoms, as well as social and property rights, so as to provide maximal protection to the individual's privacy and freedoms, Europe, with its rich philosophical tradition inherited from the Enlightenment, has enshrined a new generation of human rights ("system rights"), for organizing cyberspace.

[1] This article has been translated from French by Noal Mellott (Omaha Beach, France). The translation into English has, with the editor's approval, completed a few bibliographical references. All websites were consulted in June 2021.

[2] The GDPR: "Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data" available via: http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1478961410763&uri=CELEX:32016R0679.

The GDPR has taken shape around three major axes:

● consolidation of citizens' rights in Europe both qualitatively (with the possibility of better understanding and controlling how personal data are put to use) and quantitatively (through new rights, such as the portability of personal data);

● a new rationale for holding accountable all actors that process the data of European citizens, regardless of their location, thus placing on an equal footing all European and international entities with regard to the applicability of the law; and

● the reinforcement of sanctions by the national commissions in Europe that oversee digital technology and freedoms (the equivalent of the CNIL in France: Commission Nationale de l'Informatique et des Libertés). These sanctions have been raised to €20 million or 4% of a firm's sales worldwide.

Europe has thus provided a modern, innovative response to the problems related to the uses of personal data. The values of confidence and transparency have thus become the keystone of economic regulation and the cornerstone for the rollout of digital technology in all spheres of human activity.

New regulatory mechanisms Europewide: The consequences for firms

To avoid the risk of "forum shopping" by litigants, which might have watered down the application of regulations in cyberspace at the turn of the century, the GDPR has set up an original mechanism of network cooperation with national authorities, a sort of decentralized integration that implies deep changes in the methods of work adopted by national authorities. Firms now benefit from a "one-stop-shop mechanism", the one-stop shop being the data protection officer in charge of the firm's principal establishment. For citizens, this mechanism is their country's data protection authority. Since a firm now has a single contact among national authorities, the decisions affecting it are made in common so that the decisions formulated apply to whole European Union. If these national authorities do not agree, the European Data Protection Board (EDPB, a new institution) serves as arbitrator.

The GDPR represents a major challenge for firms. How to comply with it given the lack of any single all-purpose solution? Solutions must be adapted to each sector of business and line of trade. This entirely new role of "evangelization" has been assigned to the data protection officer in charge of assisting the firm in shifting its general position (in application of the principle of responsibility) so as to always be sure that the policies and procedures surrounding technological innovations remain valid over time and at all levels. A new lever provided by the GDPR is the principle of data protection by design and by default. It implies taking privacy into account far upstream in the drafting of programs by adopting preventive measures or making technological choices that will limit the eventuality of data violations.

This ethical requirement for a global, dynamic compliance might entail major investments in terms of funds and human resources. However these principles have become familiar in France since the passage, forty years ago, of the 1978 Act on Informatics and Freedoms. Furthermore, they might be a vector of growth for firms, who will be able to reassure their customers about the uses, quality and relevance of the data collected. For firms, data protection is now a subject of governance at the junction of the fields of computer science, the law, commerce and communications.

Having stated these grounds, we face several questions. How to generate a "collective" responsibility on par with the regulation? How to fill the GDPR's promises and make it shine brighter? What is the bottom line three years after this regulation went into effect?

An assessment three years later

France

The implementation of this new model has moved beyond the initial stages in France, as statistics show.

The GDPR has wrought its effect in professional circles. More than 24,000 data protection officers, representing more than 72,000 organizations, were declared by the end of 2020. There have been nearly 6000 notifications of violations related to personal data since 2018: approximately 1200 in 2018, 2300 in 2019 and more than 2500 in 2020. This has enabled the CNIL to better orient its advice and enforcement actions, and better play its role in the cybersecurity ecosystem.

For private persons too, the GDPR has had effects. The total number of visits on the CNIL's websites (queries and consultations of the questions/answers available on line) has sharply risen: 60% since 2018. This is a good indicator of the need for information about the GDPR. The CNIL received 14.137 complaints in 2019, a record that represented an increase of 27% compared with 2018 and of 79% over the preceding five years. The consolidated statistics for 2020 are not yet available at the time of writing, but we can be sure that the number of complaints has continued growing and that the main focus of requests was on information related to the health crisis. These increases shed a stark light on the population's everyday problems. The French have three major preoccupations:

- retain control over their data and keep them from being processed without informing the person(s) concerned. This is evinced by a 13% increase in complaints about delisting.
- not to be disturbed, but to be heard and listened to: 15% of complaints have to do with advertising, whether from businesses, associations or political groups.
- see to it that rights are upheld in dealings with employers or public services. The number of complaints related to health records increased 42%.

The CNIL carries out an average of 300 formal controls per year. The number of corrective measures has increased every year. Initially, the CNIL concentrated on educational actions that targeted economic agents. These actions involved a close dialog with network heads on the subject of monitoring and developing the tools (available on the CNIL's website, such as MOOC GDPR for very small, small and medium-sized firms) for making compliance easier and analyzing the GDPR's impact. This transition period having come to an end, the CNIL started applying sanctions: approximately fifteen in 2020 that totaled nearly €139 million (as compared with eight in 2019). The new amounts for fines set by the GDPR have come into effect.

Europe

At the European level, cooperation has become an everyday activity for regulatory authorities. More than 1300 crossborder cases have been identified, 450 so-called "one-stop" procedures have been pursued; and more than 150 final decisions, issued in application of the provisions in favor of cooperation and coherence. At the end of 2020, the EDPB adopted its first binding decision while arbitrating a dispute between Irish and other European authorities with regard to Twitter. It also adopted about twenty guidelines on topics related to the application of the GDPR, ranging from its territorial scope through targeted uses on the social media to privacy by design. This is contributing to a genuine legal doctrine on data protection in Europe.

Although the EDPB has not kept official statistics on the number of sanctions Europewide, some private websites reported that, by the end of November 2020, approximately 420 sanctions had been issued, amounting to more than €260 million in fines.

The world

Even worldwide, there has been a before and after 25 May 2018! The GDPR's extraterritoriality, which places international and European entities on an equal footing, has, along with the free circulation of data, sent strong signals about the determination to achieve European sovereignty in cyberspace. This is a matter not of protectionism but of the assertion of a regulatory model based on cybersecurity and a defense of people's rights in relation, in particular, to the GAFAM (Google, Apple, Facebook, Amazon and Microsoft). While we must avoid crowing too loudly, the GDPR has, in fact, become a source of inspiration worldwide.

Some countries have updated their regulations on data protection in order to continue trading with Europe. Such is the case of Japan, South Korea, Benin and Australia, and legislation is under way in Switzerland, Tunisia and Burkina Faso. Other countries have, for the first time, adopted a general legal framework on the processing of personal data, and the principal measures are close to those foreseen by the GDPR. Such is the case in California (the Consumer Privacy Act adopted in October 2018 and in effect since 1 January 2020) and Brazil (Lei Geral de Proteçao de Dados adopted in 2019). In India, where the Supreme Court recognized in 2017 that the right to privacy is a fundamental human right, a bill of law is under discussion in parliament. The GDPR has thus become an instrument of "soft power" in "data diplomacy".

Current issues in 2020, a test year

Several case studies were carried out in 2020 to see whether the measures foreseen by the GDPR have been applied. The year that has just ended could be a tough period for testing.

The lessons drawn from the COVID pandemic

As one of its consequences, the pandemic has focused public debate on the protection of fundamental freedoms and personal data. Major points of tension have arisen that might shift perceptions of, and preoccupations about, the protection of privacy. The CNIL has drawn several lessons from this experience.

First of all, the principles laid down by the GDPR have proven very robust. They have made it possible to avoid misuses of the legal framework on the uses of sensitive data. They have also proven flexible enough to enable member states to process data and share information under exceptional circumstances. Specifically, the principles of finality (Is the purpose of data collection clear and precise?), of necessity (For which uses?), of proportionality (Is a less intrusive means possible?), of minimization (Are only the necessary data collected?) and of a limitation on storage (Will the data be deleted once processed for the stated purpose?) have been key elements for building confidence in data processing during an emergency. They will continue serving as a guide for decisions in a post-Covid world. This emergency has clearly proven the worth of preventive approaches "by design", which various project leaders have endeavored to integrate in their data management protocols.

Secondly, the regulatory authority's role of monitoring and control has proven indispensable for holding parties accountable. The CNIL's actions in providing guidance to public administrations and private firms, and, too, upholding freedoms and privacy have proven essential for its monitoring of public authorities and private entities. For the CNIL, it is, therefore, worthwhile to communicate regularly about its legal doctrine so that these parties can adapt their plans and projects to it.

Challenges on the European scale

Other major events during 2020 have also been important for the economy, among them: the Schrems II decision whereby the Court of Justice of the European Union abolished the Privacy Shield, which allowed for data transfers between Europe and the United States; the engagement to transfer the hosting of Microsoft's Health Data Hub toward a European platform within two years; European legislation on the single market (Digital Governance Act, Digital Services Act and Digital Markets Act soon to be followed with the Data Act); and France's plans for stimulating its economy.

This exceptional context has led to an unusual alignment of interests between regulatory and industrial policies. We should seize this opportunity for pursuing an ambitious policy in view of European digital sovereignty. Upholding the GDPR will be a key to success.