The EU's General Data Protection Regulation at the service of cybersecurity

Jean Lessi,
Commission Nationale de l'Informatique et des Libertés (CNIL)

Abstract:
Whether for physical persons, private and public organizations, or society as a whole, the application of the EU's General Data Protection Regulation (GDPR) definitely expresses the determination to make personal data secure. How? By establishing specific procedures that data security organizations have to follow (notifying regulatory authorities, informing individuals), by completing the security obligations instituted in 1978, and by more heavily sanctioning violations. Beyond its provisions, the GDPR has spinoffs: a rising public awareness of data protection and of the need for digital literacy. Now to provide the means for achieving the GDPR's ambitions…

Cybersecurity, the first among digital freedoms? It is probably not the right time to hope that this formulation in terms of fundamental freedoms will have as much success in the digital realm as its predecessor has had in the physical world. The first among freedoms in the information era is, more than ever, the right to privacy and to control the uses of one's personal data. As we know, individual freedoms are frail in the absence of appropriate security measures and, even more, of a deeply shared "cybersecurity culture".[1]

The same battle: Cybersecurity and the protection of individuals

Cybersecurity is not what first comes to mind — and thus onto the agenda — from the perspective of individual rights and freedoms, but instead from the angle of the interest of organizations, indeed their vital interests. What comes to mind first of all is the interruption of activities and, thereafter, the risks of breaches of information. Information, whether state or trade secrets, has to be protected against threats of blackmail or from economic espionage. Up to this point, nothing new under the sun during our digital era. Since the turn of the century however, databases with personal information have an ever larger place in our legacy of information. As the breeding ground of the digital economy, these databases, the elementary particles of many a commercial activity, have become a highly valued strategic asset.

This is the point where the rights of individuals and the interests of data-processing organizations meet. We might think this is a chance meeting. On the contrary, the two are inherently linked. A breach of data simultaneously affects two categories of victims: physical persons and (private or public) organizations.

[1] This article, including quotations from French sources, 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 March 2020.

For individuals, a breach of their data is a violation of confidentiality with the pure and simple risk of a disclosure of their privacy and subsequent threats of blackmail, phishing or even an usurpation of identity. This has a quite real psychological impact. When there is a violation of the availability or integrity of personal data (*e.g.*, the data transferred to third parties as might happen when uploaded photographs or medical records vanish from an online service), individuals lose, to various degrees, control over their private lives.

For organizations, a data breach is an infringement on their reputation and sometimes represents an economic dead loss (*e.g.*, the cybertheft of $101 million in 2016 from the Bangladesh Bank). No organization comes unscathed out of a security incident that has affected its data protection. There is the harm to its image and reputation once the incident receives publicity. Events regularly remind us that keeping an incident secret is neither recommended nor, sometimes in practice, possible; nor, for that matter, legal in certain cases.

As we have seen, organizations and physical persons are but two sides of the same coin. This also holds with regard to the security of legacy data, since we try in vain to tell the difference between data that are and that are not "personal". The two often overlap, thus requiring for a common approach. What characterizes the recent trend in our digital economy is that this overlapping is more and more systemic. An incident is seldom restricted to a face-to-face relation between an organization and a person. Incidents usually involve files or entire databases. An attack can affect hundreds, thousands or even millions of people. More broadly, the combination of the quantity, accuracy, variety and wealth of the data processed — whether data collected initially, the data produced by the individual's online activities or the data from operators — has turned the security of legacy data into an absolute condition for building up citizens' confidence in the digital economy's very foundations.

For these reasons, cybersecurity is the keystone of online business models. As much can be said about the new models that, developed for public administrations since the 1990s, are based on processing personal data alone. On the one side, this legacy of data is cumulative, enriched, massified. On the flip side, physical persons have to have confidence that organizations are capable of processing their data as promised and that the data entrusted to an organization for storage will not be lost. The equation hardly becomes simpler when we focus on the many centrifugal forces in our digital economy: international transfers (from one point to another along with subsequent transfers), multiple intermediaries in a chain (sometimes complex and opaque) of subcontractors, cloud storage, etc.

Le GDPR, a powerful cybersecurity tool

The French Act of 6 January 1978 on "*Informatics and Freedoms*" did not have the reputation of being a cybersecurity tool; but it would very much prove to be so. Article 29 already provided: "*Any person ordering or performing a processing of nominal information is, by this fact, committed toward the persons concerned to take all precautions useful for preserving the security of the information and, in particular, to keep them from being distorted, damaged or communicated to unauthorized third parties.*"[2] Everything was in this act: the obligation of security along with its definition and motivation (namely: the confidence of those who entrust their data to the party who accepts them). In fact, security was already omnipresent in the controls performed by the CNIL (Commission Nationale de l'Informatique et des Libertés) and the sanctions administered. From year to year, at least 80% of these controls concerned lapses in security obligations; and a majority of the sanctions decided each year by the CNIL in nonplenary meetings targeted violations of this sort.

[2] Act n°78-17 of 6 January 1978 on Computer files and freedoms (consolidated on 13 March 2020) available at https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000886460&fastPos=2&fastReqId=2121642886&categorieLien=cid&oldAction=rechTexte. Texts of French laws and decrees, as well as many court decisions, are available at https://www.legifrance.gouv.fr/Droit-francais.

We must, nonetheless, admit that this act of law from 1978, though ahead of its times in some ways, failed to create the electroshock needed to raise the level of security in French organizations, public and private. In continuity with this French act, the EU's General Data Protection Regulation (GDPR), enforced since 25 May 2018, must now concretely meet up to its promises.

In effect, the GDPR has retained the obligation of security and, without modifying its substance, has broadened its formulation. While sparing the details, let us mention: the emphasis (Article 35) on "*the necessity and proportionality of the processing operations*" to the actual nature and intensity of the risks in each context; the explicit mentioning of encryption as a tool; the GDPR's very broad approach to the concept of security as the "*ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services*" (Article 32); etc. Nothing therein is alien to the CNIL's doctrine under the French act of 6 January 1978. But everything has now been set down in writing.

An innovation under the GDPR is the much heavier sanctions. Depending on the stakes, the sanction for a failure to meet the obligation of security may amount to 2% of "*total worldwide annual turnover*" (Article 83) or €10 million, the higher of these two options being applicable.

The GDPR thus makes the security obligation, which previously existed under French law, more credible. By taking into account the complexity of data-processing operations, it lays down specific requirements (in particular with regard to security) for subcontractors and sets the sanctions, whereas the French act recognized a single party: the head of data-processing. This did not mean that subcontractors had no liability before 25 May 2018, but it was indirect, and mainly contractual or commercial. Henceforth, Article 28 of the GDPR specifies the contents for data-processing contracts; and subcontractors are liable to regulatory authorities or eventually judges for lapses in security obligations.

However the GDPR's major innovation is in cybersecurity. It concerns the many procedures which place the obligation of security at the center of governance in organizations and remind them of this obligation. For example, the measures related to data breaches advance in three steps as a function of the degree of risks to the rights of persons. If a breach has occurred that carries no risk, the person in charge of data-processing need but record it in an in-house registry. If the breach entails risks, he has to, in addition, notify the incident to the CNIL as soon as possible (72 hours at most). If the breach entails a high risk, he has to notify the persons whose data were affected as soon as possible. The organization may postpone this latter notification (but not the notification to the CNIL) if necessary, for example because an operation of cyberdefense has been launched or an investigation opened about the origins and channels of the attack.

This new "security discipline" is gradually being tightened. During the first year of enforcement of the GDPR, the CNIL received more than 2000 notifications of violations, compared with approximately 89,000 at the EU level (with strong variations among member states). The discipline related to the three aforementioned steps has three positive effects:

- upgrade the cybersecurity skills and qualifications of organizations while motivating them to strengthen controls and learn to react to incidents;
- protect the physical persons affected by data breaches from subsequent risks (phishing, for example); and
- internalize the systemic nature of cybersecurity, which links an organization to all the physical persons whose data are processed by it, and see to a proportionality between the data-processor's obligations and the risks caused for the parties whose date have been breached.

The GDPR requires a "*data-protection impact assessment*", another security procedure, prior to the processing of data with a high risk for the rights and freedoms of individuals. This assessment analyzes risks and formally evaluates the impact on persons and firms. It has to include an action security plan and a principle for making ongoing improvements. Once again, the obligation related to the procedure and method is intended to foster the right questions, the right reflexes and the right solutions so as to ultimately better protect (and therefore better process) personal data.

The GDPR and cybersecurity: From the legal text to public policies

A text of law does not make a public policy. As a driving force, along with other institutions, for a public policy in cybersecurity, the CNIL intends to transpose the GDPR's text into actions. It will thus help raise, by one or two notches, the level of collective cybersecurity in France. After all, the initial level can, to be polite, said to be in want of perfection.

First of all, the discourse about cybersecurity must be such that all organizations, big and small, are capable of hearing it. As for the protection of personal data, experience has shown that points of vulnerability, given how numerous they are, can be effectively handled only by mustering the whole business and administrative environment. Cybersecurity must thus be "democratized" so as to reach down into small and medium-sized firms, small public administrations and even NGOs. The CNIL proposes special tools for them. A handbook for small and medium-sized firms (drafted along with the Public Investment Bank) and a handbook for raising the awareness of local authorities are in line with the editorial work done by ANSSI, which has published (in partnership with the CPME) guidelines of good practices for information systems. The CNIL is preparing educational materials (such as a simplified registry of data-processing operations). This orientation will be maintained in the coming years, perhaps in new forms (recommendations, standardized rules, etc.). Being educational is not just a matter of words. Handy electronic tools must be made for practical exercises. The CNIL has equipped its handbooks with free, open-source software (available in 18 languages).

Secondly, the public must be informed about cybersecurity; and its skills, upgraded. We cannot rely on organizations alone; individual citizens have their own share of responsibility. Without being pessimistic, it should be pointed out that the systemic nature of risks during the information age requires mobilizing, with seriousness and determination, all of society to address this issue together. Education in digital technology, in all facets, is a full part of this undertaking: education about the issues underlying the digital economy, about right and wrong online practices, and about the reflexes to adopt to safeguard privacy (one's own and others') on the Web. The CNIL and members of Educnum are undertaking educational actions of this sort.[3]

The enforcement of the GDPR makes a big step forward toward raising the level of cybersecurity in France and Europe. This will not do everything. But beyond the obligations related to it and the procedures created by it, the GDPR has laid a cornerstone for a public cybersecurity policy. It is time to gauge how issues in this field overlap for citizens and for organizations, and to meet up to expectations.

[3] For instance, "10 conseils pour rester net sur le Net", a video made by Le Rire Jaune (a YouTuber) in partnership with the CNIL and MGEN: https://www.cnil.fr/fr/10-conseils-pour-rester-net-sur-le-web.