The user,
a stakeholder in data regulation

Isabelle Falque-Pierrotin,
president of the Commission Nationale de l'Informatique et des Libertés (CNIL)

Abstract:
Since 25 May 2018, the European Union has a new legal framework for the regulation of personal data, the General Data Protection Regulation (GDPR), designed with the ambitious objective of placing users back into the "equation" of the promises proffered by digital technology. This intervention by EU lawmakers was timely. Within a few decades, as personal data have become increasingly important in economy and society, individuals feel ever more dispossessed, an anxiety related to the complex digital ecosystem. The Internet has been built around the idea of emancipation; but breaches of security and successive scandals with violations of personal data reinforce the impression of a fragile, dubious infrastructure, over which the individual no longer has any control. By enabling individuals to better control their lives on line, the GDPR is a crucial step toward placing users at the center of the digital "story". It endows them with an unprecedented sovereignty over their own data and enables them to re-exercise free will in the digital realm. Thanks to the GDPR, the law has managed to embrace the digital practices of the 21st century while reasserting the fundamental values anchored in European humanism. The coming months are critical. Users, firms and regulatory authorities will, as they make the GDPR operational, be accountable for its results. Avoiding a dispossession caused by digital technology is still a subject for ongoing discussion at a time when big regions in the world are vying for digital sovereignty and when data analytics and artificial intelligence are making strides.

Initial assessment: Dispossession and loss of confidence

The Internet has been built on a promise to individuals, the promise of emancipation from authorities in the physical world who were deemed to be out of phase with the new reality of technology.[1] In his declaration of independence of cyberspace, John Perry Barlow (1996) declared freedom and self-determination to be the key principles for organizing this new world. This original political positioning of digital technology around individuals as such and their freedoms was based on a technical infrastructure that placed computer intelligence on its periphery in order to favor the rapid development of new uses.

The processing of personal data seemed, at first, to be in line with this trend. Services became more and more personalized; and this customization has continually augmented and gradually gained ground in all areas of our lives: commerce, medicine, social relations, culture. All these advances feed on personal data, which are used to propose services, ever more efficient and ever better targeted as a function of users' profiles.

Individuals have imperceptibly lost control, as consumers or users in the digital economy. Although the person's "informational halo", the pool of data describing him or her, is used to provide better service or even predict needs, individuals might feel locked in by this extrapolation from their past choices or by the model used to build the personalized offer made to them. Furthermore,

[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.

individuals are ever more helpless when faced with the terms of use for the proposed services or when browsing the ecosystem underlying the digital economy. It was already hard for most users to form a clear idea about cookies, let alone grasp their business implications. Meanwhile, cookies have become much more obscure with the growth of online advertising and market shares. Very profitable businesses have sprung up to capture the attention of cybernauts by using various techniques to orient them toward, or keep them loyal to, an application, a website, a content. Ultimately, the figure of the triumphant user on the Internet has been replaced with that of an individual, placed in a category, calculated, and, according to some critics, manipulated. What has made all these changes possible is the ever more powerful tools used for data analytics and processing along with the continuous expansion of the data used.

Several recent events have placed the spotlight on this previously rather confidential disequilibrium. Edward Snowden's revelations in 2013 signaled a turning point. They revealed that acts of intrusion and surveillance via personal data were not related to national security issues alone; nor were they a matter of concern just for those who wanted to keep their secrets hidden. Instead, as Snowden realized, each citizen was likely to come under mass surveillance. This attested to a sort of alliance between private organizations' gigantic databases and public officials' security objectives. Individuals had, once again, the impression of being objects in a complex informational infrastructure. The citizen's disillusion accumulated with the consumer's disappointment.

In all countries, apprehension arose — a crisis of confidence in digital technology. The lack of data protection was crystallizing anxieties, which were regularly riled by a string of masterly security breaches reported on news programs.

The GDPR: Users at the center

In response to this assessment and crisis of confidence, the EU's General Data Protection Regulation (GDPR) — adopted in 2016 and enforced as of 25 May 2018 — proposes a regulatory model for establishing a new balance in the asymmetrical relation between individuals and data processors.[2] It seeks to place the individual at its center. Underlying this very strong political message are the wagers: that technology and innovation cannot develop at odds with users, that Europe will gain a genuine competitive advantage by using the law and ethics; and that technology, while creating new possibilities, should not impose a vision of the future that overlooks our freedoms.

In concrete terms, the GDPR's 99 articles and 173 recitals seek, through a full set of new procedures and obligations, to make those who collect and process personal data responsible for protecting the data. Firms, in particular, are to take account of the protection of personal data during everyday operations. The GDPR also rearms individuals for a dialog with digital technology; it lets them manage their digital lives by using their own criteria. Furthermore, this protection extends beyond Europe's borders since global players, even those not installed in Europe, are subject to EU law once their products or services target the EU market.

For users, the GDPR reinforces their rights, in particular the right to consent to the collection and use of their personal data. Consent must now be freely given specific to the use with conditions "*using clear and plain language*" and "*with the right to withdraw consent at any time*" (Art. 7). In other words, users ("*data subjects*") must be able to understand the processing of their data, freely choose to accept it or not, and freely change their minds. Furthermore, they gain more control since they are now able to invoke a "right to be forgotten", *i.e.*, to have their data erased, so that their digital past not catch up with them (Art. 17). The GDPR's ambitious goal coincides with users' expectations.

[2] The GDPR (General Data Protection Regulation): "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.

One of the GDPR's more innovative measures for making users active is the new "*right to data portability*" (Art. 20). Certain data (*e.g.*, play lists, journals of events, such as the orders recorded on a customer's loyalty card) are to be retrievable in an easy-to-reuse form so that, if need be, they can be transferred to a third party for reuse in a new context. This gives a real advantage to European consumers. The latter can take back power by turning toward services that prey less on their data; and they can thus reduce the asymmetry that used to turn to their disadvantage. Another interesting point is that this new right focuses on a specific aspect of the digital transition, namely: personal data, which are becoming an asset to control and promote rather than a stock of information to be protected. The user's participation will, in the coming years, increasingly involve adopting an active, dynamic — and not just defensive — stance.

The GDPR seeks to help users take their digital lives back into their own hands. The new arrangements for European cooperation foreseen under this regulation do not create a new administrative burden on users. The user's one-stop contact is his/her national data protection authority, even in cases of crossborder data processing (under the conditions set in Art. 4.23 and assuming that it is not the supervisory authority of the processing). Another major advance in the exercise of digital rights is the reinforcement of the means for joint actions. A new right to compensation is foreseen for anyone morally or materially harmed by a violation of the regulation. Victims used to be atoms dispersed throughout the digital realm; but they will now be able to obtain redress through a joint court action undertaken by not-for-profit organizations.

In summary, the GDPR's intent is to make it possible for individuals to rediscover a sort of sovereignty over their data, since this is the price to be paid for the ongoing development of digital technology and a robust digital economy. However this moderate, balanced approach does not force personal data into a regulatory straitjacket that would tie the hands of innovation. For example, the regulation foresees other legal grounds than consent for collecting and using personal data. Nor does the GDPR outlaw the formation of data warehouses for the development of research and artificial intelligence in Europe.

Making the law operational in the coming years: Active, aware digital citizens

Having chosen to be realistic about data protection, the European Union relies on an ethical rather than a purely market approach or on mass surveillance (as in certain rival models). It wants to make its voice clearly heard about the major issue of the 21st century, namely the building of a digital society.

However the law might sometimes have trouble reaching its target. Persons from English-speaking lands frequently address this criticism to Europeans: "Your system is ethically superior, but it is an unoperationalized dead letter." After the first months of enforcement of the GDPR however, we predict that this regulation will reach its target. The number of complaints filed during the first few months with European data protection authorities has risen significantly: in France for instance, an increase of 64% during the first four months. Associations have already resorted to the possibility of joint actions. Individuals have seized on the new rights offered by the GDPR: they invoke them with data processors and count on regulatory authorities to uphold them. A "digital culture" is gradually being built, this time under pressure from users.

To follow up on this new social demand, the CNIL (Commission Nationale de l'Informatique et des Libertés: National Commission on Informatics and Liberty) is tapping educational resources. The GDPR has been the occasion for overhauling our website, enhancing FAQs, and proposing new online services (for filing complaints, notifying violations, etc.). A MOOC will soon be available to professionals. These long-term educational actions have to be conducted as part of a general push for fostering the citizen's digital maturity. The CNIL has the drawn attention of the ministries of Education and of Higher Education to this. Since 2013, it has brought together approximately seventy

quite different people from education, research, the digital economy and "civil" society (corporate foundations and other institutions) in Educnum.[3]

The CNIL will also have to prove to plaintiffs that European cooperation is operational in this new field, that regulatory authorities are actually able to apply a common set of sanctions to big transnational firms in the defense of citizens' rights. This issue is sensitive: national authorities are not used to cooperating and have to learn how to oversee networks, share operational skills with each other, and make joint decisions on crossborder questions. The GDPR's credibility hinges on this.

In the mid-run, the GDPR could affect the whole ecosystem. Pressure from citizens and consumers is reshaping the market. However it must be not only reactive but also offensive. It has to allow for new economic and industrial models of privacy protection to emerge. The GDPR is a lever for social innovation, a major opportunity for turning privacy into an argument that firms can use to compete for customers. The right of data portability, for example, could be a tool for groups to collectively gain more control by making their data available for projects in the general interest, which public organizations choose and conduct. The CNIL's smart city report (LINC 2017) and the strategy for artificial intelligence (Villani 2018) have underscored this "citizens' portability". The CNIL wants to contribute to these debates and experiments through prospective activities for deploying a "start-up strategy", which offers legal security to start-ups in the digital economy, and for proposing "service regulations" for firms (specifications for certification, codes of conduct, etc.).

Beyond being a field of data harvested for advertising, active users have a future; and the GDPR has opened the way.

Algorithms and artificial intelligence, the end of the active individual?

Algorithms and artificial intelligence (AI) have raised new issues about individuals taking back more control over their digital lives. Owing to the progress in algorithms and big data, considerable advances have been made in predictive models. The conditions for decision-making in this new age of technology are changing. Are users capable of understanding the black box of algorithms — how algorithms have "calculated" the results, or even how they sometimes discriminate against users? Following a lively public hearing on algorithms and AI, the CNIL (2017) proposed an action plan for following up on this powerful technology's ethical development. As this plan stated, substantial progress is yet to be made in organizing the "accountability" for these new tools. One possibility would be to make it easier to understand algorithmic systems by improving mediation with users; another would be to promote design-based solutions for understanding the promise held by algorithms and adjusting them to one's own needs.

In general, end users of AI are a full-fledged part of the "algorithmic chain" and, for this reason, ought to be associated with the sorts of regulation to be imagined. But is this possible? For some observers, like the historian Yuval Harari, it is too late: our free will has reached a dead end, since external factors beyond our control determine our choices. The autonomous individual, the very grounds of human rights, is now nothing more than an illusion. Since individuals will inevitably feel more and more useless, being an "active" user of AI is an oxymoron.

Notwithstanding this, the challenges from recent trends in technology (starting with AI) might be arguments for a new approach that will allow individuals to find their place in the ecosystem. If free will is tailing off — if certain initial rights that have been shielded over the centuries seem to be dwindling as AI arises, enclosing us, discriminating among us, disempowering us — might it not be time devote thought to new principles of governance for reviving these rights? The time has come

[3] https://www.educnum.fr/fr/le-collectif-educnum

for us to imagine new personal rights for this new era. In its report, the CNIL (2017) has called for "infrastructure rights" or "system rights" for organizing the digital realm's underlying dimension.

When the human adventure advances from one phase to the next, a vision of the individual is constructed: at first, the individual in relation to him/herself; then, over the centuries, a slow transition from a determined to an emancipated, universal individual endowed with strong civil and political rights; then the individual in relation to contemporaries, a vision that resulted in adopting "social rights" for bridging the gap between formal and real freedom in a context of economic upheaval; and finally, the individual as a collective being linked to the environment and future generations through rights and "solidarity". Yet to be constructed is a vision of the individual's position in relation to the informational infrastructure, to the algorithmic digital technology that, sometimes invisibly, surrounds, overhangs and crosses our lives.

The international adoption of the principles of loyalty and vigilance for AI systems, which the CNIL has proposed, could fit into this vision. The preservation of pluralist sources of information is one example, given the political campaigns targeting individuals on the social media. Loyalty is toward not only the users of clearly defined AI-based services but also, and above all, toward communities of individuals (or a much larger set of collective interests affected by this technology). Vigilance means methodologically organizing our attention so that free will can ultimately still have a meaning at a time when the compartmentalized rollout of AI in our lives seems likely to lead to collective disempowerment.[4]

Conclusion

In a world where we learn, day after day, a little more about what can be done with our personal data, the GDPR seeks to give back to users control over their digital lives. Europeans now have the possibility of being better protected and empowered to cope with digital technology than people in any other region in the world. Rather than "accepting it all" (and giving up our freedoms) or "sacrificing it all" (and forgoing the promises of digital technology), the GDPR advocates a "middle way" for citizens to have a choice, a control, and access to a form of accountability — the possibility to continue benefitting from digital technology (creating relations through the Internet, exposing one's self on the social media, using personalized digital services, etc.) without being, at the same time, forced to entertain close relations with the organizations that collect our data. Regulatory authorities will have the serious task of maintaining this equilibrium as technology evolves.

[4] These principles are to come under discussion at the International Conference of Data Protection and Privacy Commissioners (ICDPPC).

References

BARLOW J.P. 1996 “A declaration of the independence of cyberspace” (San Francisco, CA: Electronic Frontier Foundation) available at https://www.eff.org/cyberspace-independence.
CNIL [Commission Nationale de l’Informatique et des Libertés] (2017) *Comment permettre à l'homme de garder la main? Les enjeux éthiques des algorithmes et de l'intelligence artificielle*, December, 80p. Available via
https://www.cnil.fr/sites/default/files/atoms/files/cnil_rapport_garder_la_main_web.pdf.
HARARI Y.N. (2018) *21 Lessons for the 21st Century* (New York: Spiegel & Grau).
LINC [Laboratoire d’Innovation Numérique de la CNIL] (2017) “La plateforme d’une ville. Les données personnelles au coeur de la fabrique de la smart city”, *Cahier IP (Innovation et Prospective)*, 5, pp.1-54. Available via https://www.cnil.fr/sites/default/files/atoms/files/cnil_cahiers_ip5.pdf.
VILLANI C., (2018) *Donner un sens à l'intelligence artificielle. Pour une stratégie nationale et européenne* (Paris: Prime Minister’s Office), 235p. Available via:
https://fichiers.acteurspublics.com/redac/pdf/2018/2018-03-28_Rapport-Villani.pdf.